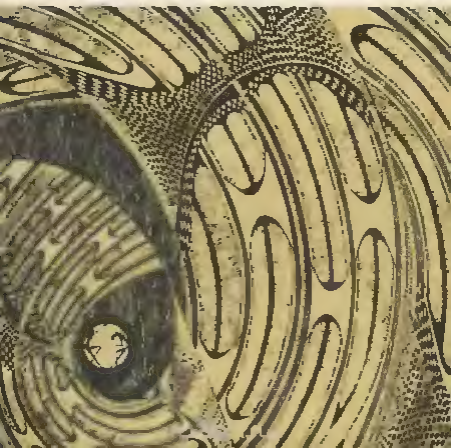
Н. КОБЛИЦ

p-АДИЧЕСКИЕ ЧИСЛА, p-АДИЧЕСКИЙ АНАЛИЗ И ДЗЕТА-ФУНКЦИИ



Graduate Texts in Mathematics

58

NEAL KOBLITZ

p-ADIC NUMBERS, p-ADIC ANALYSIS, AND ZETA-FUNCTIONS

Springer-Verlag
New York Heidelberg Berlin
1977

«Современная математика»
Вводные курсы

Н. КОБЛИЦ

p-АДИЧЕСКИЕ ЧИСЛА, p-АДИЧЕСКИЙ АНАЛИЗ И ДЗЕТА-ФУНКЦИИ

Перевод с английского
В. В. Шокурова

под редакцией
Ю. И. Манина

Издательство «Мир»
Москва 1982

ББК 22.132
К 55
УДК 517.1

Коблиц Н.

К 55 p-адические числа, p-адический анализ и дзета-функции. Пер. с англ. В. В. Шокурова / Под ред. и с предисловием Ю. И. Манина. — М.: Мир, 1981, 192 с., ил.

Вводный курс по p-адическому анализу — объекту многочисленных исследований в теории чисел, теории представлений групп, алгебраической геометрии, который служит связующим звеном между непрерывной и дискретной математикой, написанный с большим педагогическим мастерством молодым американским математиком.

Для студентов-математиков младших курсов университетов и пединститутов.

К $\frac{20203-012}{041(01)-81}$ 12—81, ч. 1 1702030000

ББК 22.132
517.1

Редакция литературы по математическим наукам

© 1977 by Springer-Verlag, New York Inc. All rights reserved. Authorised translation from English language edition published by Springer-Verlag Berlin — Heidelberg — New York

© Перевод на русский язык, «Мир», 1981

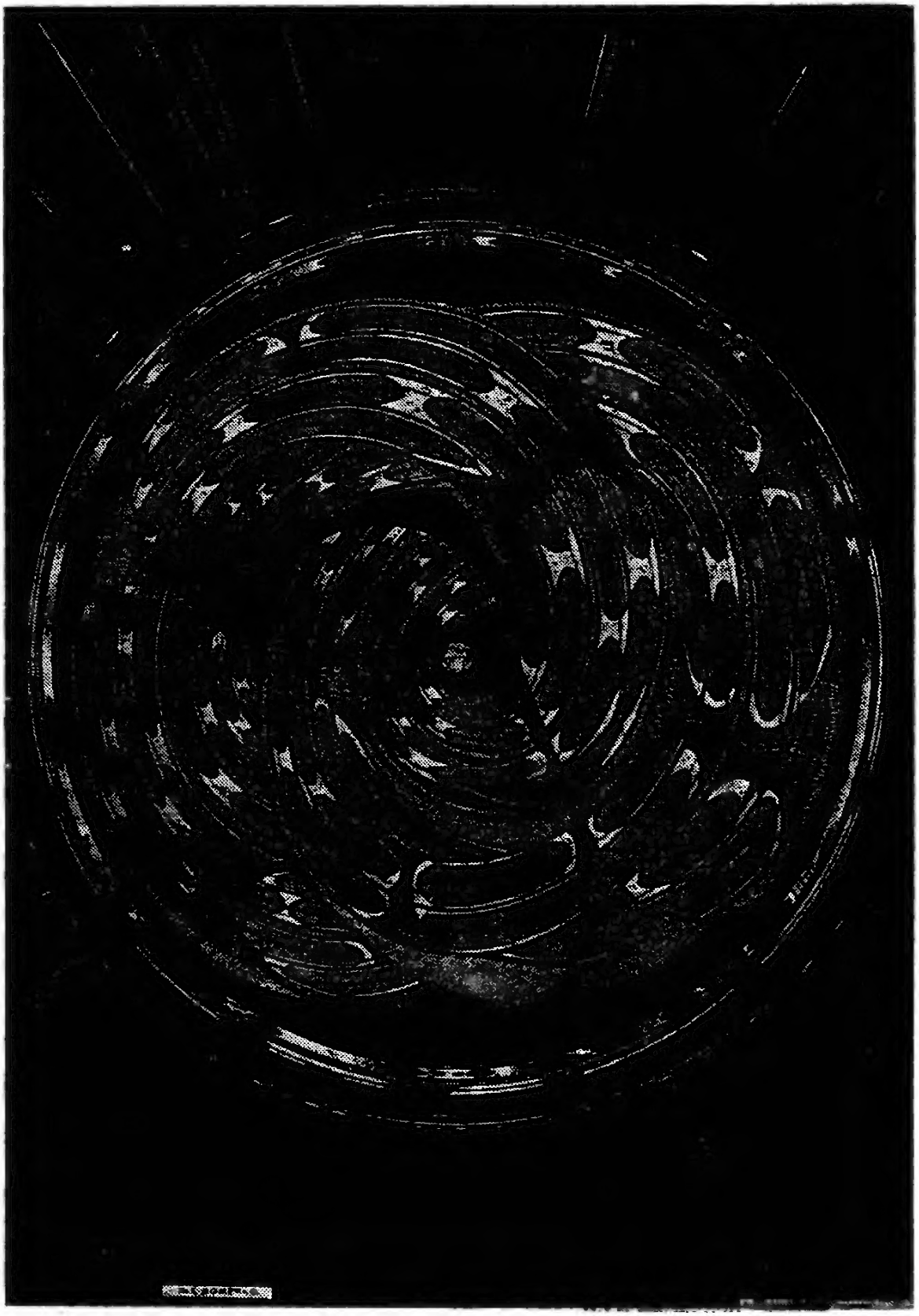
ОТ РЕДАКТОРА ПЕРЕВОДА

Вещественные числа — это пополнение поля рациональных чисел в обычной топологии. Давно известно, что у поля рациональных чисел есть еще много топологий, согласованных с операциями. Эти топологии нумеруются простыми числами; пополнения по ним суть поля p-адических чисел. p-адический анализ создавался медленно. Перенос обычных определений в неархимедову ситуацию кажется обманчиво простым делом, но глубокие теоремы требуют деликатных изменений в структуре основных понятий.

Книга молодого американского математика Нила Коблица — одно из немногих в мировой литературе введений в этот быстро развивающийся предмет. В ней живо, с вниманием к читателю и на содержательном материале представлены первые идеи, проблемы и методы p-адического анализа. Очевидно, что некоторые основные задачи ставит теория чисел. Два круга вопросов, относящихся к дзета-функциям алгебраических многообразий над конечными полями и к классической дзета-функции Римана, изложены в книге подробно. Ознакомившись с этим материалом, читатель сможет работать с обширной журнальной литературой последних лет, посвященной увлекательным свойствам p-адических дзета-функций.

Рисунок д-ра физ.-мат. наук А. Т. Фоменко на следующей странице (деталь — на обложке) символизирует 2-адический соленоид. Как и все графические листы Фоменко, он отличается скрупулезной деталировкой, и стоящий за ним математический образ поддается точному анализу. Читателю, который склонен к целостному восприятию, глубокая работа Фоменко напомнит о почти всегда скрытой визионерской компоненте математического творчества.

Ю. Манин



Профессору Марку Кацу

ПРЕДИСЛОВИЕ

Эти записи лекций задуманы как элементарный вводный курс p-адического анализа. По этой причине требования к подготовке читателя минимальны. Помимо трехсеместрового курса математического анализа предполагается знакомство с некоторыми более абстрактными математическими понятиями — в такой степени, чтобы читателя не испугали матрицы с элементами не обязательно из вещественного поля, расширения поля рациональных чисел или непрерывные отображения топологических пространств.

Книга преследует двоякую цель: изложить некоторые основные понятия p-адического анализа и продемонстрировать два его замечательных применения. Исторически они серьезно стимулировали интерес к предмету; я надеюсь, что они могут быть столь же эффективны с педагогической точки зрения. Первый из этих результатов использует лишь самые элементарные свойства поля $\mathbb{Q}_p$ и поэтому помещен в гл. II. Это — предложенная Мазуром конструкция (с помощью p-адического интегрирования) p-адической дзета-функции Куботы — Леопольдта, которая «p-адически интерполирует» значения дзета-функции Римана в нечетных отрицательных целых числах. При изложении я пользовался (неопубликованными) записями Мазура, сделанными для Бурбаки. Затем я возвращаюсь к основаниям: устанавливается возможность продолжения p-адической нормы на алгебраические расширения поля $\mathbb{Q}_p$, строится p-адический аналог поля комплексных чисел и развивается теория p-адических степенных рядов. При этом специально подчеркнуты аналогии и различия с привычными понятиями и примерами из математического анализа. В гл. V содержится второй основной результат: данное Дворком доказательство части знаменитых гипотез А. Вейля о рациональности дзета-функции системы уравнений над конечным полем. В этой главе я следовал изложению Серра, помещенному в одном из выпусков Séminaire Bourbaki.

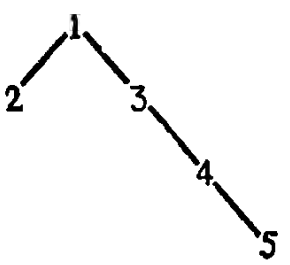
Эта книга не претендует на полноту. В ней не отражены такие темы, как теорема Хассе — Минковского (которую можно найти в гл. 1 книги З. И. Боревича и И. Р. Шафаревича [(b) 1]) и результаты диссертации Тэйта (которая воспроизведена также в учебнике Ленга [(b)2]). Кроме того, автор не пытался представить результаты в самой общей форме. Например, p-адические L-функции, соответствующие характерам Дирихле, лишь мимоходом упомянуты в гл. II. Целью автора был отбор материала для полугодового курса по p-адическому анализу, доступного второкурсникам.

Упражнения по большей части легкие, но они важны для активного овладения материалом. Кроме того, обилие упражнений позволит многим изучающим книгу овладеть предметом самостоятельно или при минимальном руководстве, проверяя и закрепляя свое понимание материала проработкой задач.

Интерес к p-адическому анализу объясняется несколькими причинами. Прежде всего p-адической технике отводится важное место во многих областях математических исследований — например, в теории чисел и теории представлений. Но немаловажно и то, что студенту, недавно познакомившемуся с рядами и интегралами, «прекрасный новый мир» неархимедова анализа представит классический анализ в неожиданном свете. Уходя корнями в классический анализ и в то же время в алгебру и теорию чисел, p-адический анализ открывает важные перспективы читателю, интересующемуся любой из этих областей.

Я хотел бы поблагодарить профессоров Марка Каца и Ю. И. Манина за их многолетнюю помощь и поддержку, а также за образцы педагогической проницательности в преподавании и изложении, образцы, которым их ученики могут ревностно подражать.

Схема зависимости глав



Глава I

p-АДИЧЕСКИЕ ЧИСЛА

§ 1. ОСНОВНЫЕ ПОНЯТИЯ

Пусть X — непустое множество. Функция d, определенная на множестве всех упорядоченных пар (x, y) элементов X и принимающая неотрицательные вещественные значения $d(x, y)$, называется расстоянием или *метрикой* в X, если она обладает следующими свойствами:

(1) $d(x, y)=0$ тогда и только тогда, когда $x=y$;
(2) $d(x, y)=d(y, x)$;
(3) $d(x, y)\leqslant d(x, z)+d(z, y)$ для всех $z\in X$.

Множество X вместе с заданной в нем метрикой d называется *метрическим пространством*. Как мы вскоре увидим, одно и то же множество X может допускать много различных структур метрического пространства (X, d).

Чаще всего в качестве множеств X мы будем рассматривать поля. Напомним, что поле F есть множество с двумя бинарными операциями $+$ и $\cdot$, такими, что F является коммутативной группой относительно операции $+$, а $F-\{0\}$ относительно операции $\cdot$, и выполнен закон дистрибутивности. Примеры полей, которые следует пока иметь в виду, — это поле рациональных чисел $\mathbb{Q}$ и поле вещественных чисел $\mathbb{R}$.

Мы будем иметь дело с метриками d, соответствующими *нормам* на поле F. Нормой называется отображение, обозначаемое через $\|\ \|$, поля F в множество неотрицательных вещественных чисел, такое, что:

(1) $\|x\|=0$ тогда и только тогда, когда $x=0$;
(2) $\|x\cdot y\|=\|x\|\cdot\|y\|$;
(3) $\|x+y\|\leqslant\|x\|+\|y\|$.

Когда мы говорим, что метрика d «соответствует» норме (или «индуцирована» нормой) $\| \|$, то под этим мы понимаем, что метрика d определяется соотношением $d(x, y) = \|x - y\|$. Легко проверить, что функция d, заданная таким образом по произвольной норме $\| \|$, будет действительно метрикой.

Основной пример нормы на поле рациональных чисел $\mathbb{Q}$ дает абсолютная величина $|x|$. Индуцированная ею метрика $d(x, y) = |x - y|$ совпадает с обычным расстоянием на числовой прямой.

Я начал с абстрактного определения расстояния потому, что отправным понятием для всего дальнейшего будет метрика нового типа. Она удовлетворяет условиям (1) — (3), но ее свойства существенно отличаются от привычных интуитивных представлений. Кроме того, я напомнил абстрактное определение поля, так как вскоре нам придется работать не только с полем $\mathbb{Q}$, но и с его различными расширениями.

§ 2. МЕТРИКИ ПОЛЯ РАЦИОНАЛЬНЫХ ЧИСЕЛ

Одну метрику с поля $\mathbb{Q}$ мы знаем: она индуцирована обычной абсолютной величиной. Есть ли еще какие-нибудь метрики? Следующее определение является основой для всего дальнейшего.

Определение. Пусть $p \in \{2, 3, 5, 7, 11, 13, \ldots\}$ — некоторое простое число. Для произвольного ненулевого целого числа a положим $\operatorname{ord}_p a$ равным кратности вхождения p в разложение a на простые сомножители, т. е. наибольшему целому неотрицательному числу m, для которого $a \equiv 0 \pmod{p^m}$. (Запись $a \equiv b \pmod{c}$ означает, что c делит $a - b$.) Например: $\operatorname{ord}_5 35 = 1$, $\operatorname{ord}_5 250 = 3$, $\operatorname{ord}_2 96 = 5$, $\operatorname{ord}_2 97 = 0$. (Если $a = 0$, то условимся писать $\operatorname{ord}_p 0 = \infty$.) Отметим, что функция ord_p немножко похожа на логарифм: $\operatorname{ord}_p (a_1 a_2) = \operatorname{ord}_p (a_1) + \operatorname{ord}_p (a_2)$.

Теперь для произвольного рационального числа $x = a/b$ положим $\operatorname{ord}_p x$ равным $\operatorname{ord}_p a - \operatorname{ord}_p b$. Так определенная величина зависит только от x, т. е. из представления $x = ac/bc$ мы получим то же самое значение для $\operatorname{ord}_p x = \operatorname{ord}_p ac - \operatorname{ord}_p bc$.

Кроме того, определим на $\mathbb{Q}$ следующее отображение $|\ |_p$:

$$|x|_p = \begin{cases} \dfrac{1}{p^{\operatorname{ord}_p x}}, & \text{если} \quad x \neq 0; \\ 0, & \text{если} \quad x = 0. \end{cases}$$

Предложение. *Функция* $|\ |_p$ *является нормой на поле* $\mathbb{Q}$.

Доказательство. Проверку свойств (1) и (2) оставим читателю в качестве легкого упражнения. Установим (3).

Если $x=0$ или $y=0$, или если $x+y=0$, то свойство (3) очевидно. Поэтому предположим, что числа x, y, $x+y$ отличны от нуля. Пусть $x=a/b$ и $y=c/d$ — несократимые представления. Тогда $x+y=(ad+bc)/bd$ и $\operatorname{ord}_p(x+y)=\operatorname{ord}_p(ad+bc)-\operatorname{ord}_p b-\operatorname{ord}_p d$. Заметим теперь, что наибольшая степень p, делящая сумму двух целых чисел, *не меньше* любой степени p, которая делит одновременно каждое слагаемое. Поэтому

$$\begin{aligned} \operatorname{ord}_p(x+y) &\geqslant \min(\operatorname{ord}_p ad,\ \operatorname{ord}_p bc) - \operatorname{ord}_p b - \operatorname{ord}_p d = \\ &= \min(\operatorname{ord}_p a + \operatorname{ord}_p d,\ \operatorname{ord}_p b + \operatorname{ord}_p c) - \\ &\qquad - \operatorname{ord}_p b - \operatorname{ord}_p d = \\ &= \min(\operatorname{ord}_p a - \operatorname{ord}_p b,\ \operatorname{ord}_p c - \operatorname{ord}_p d) = \\ &= \min(\operatorname{ord}_p x,\ \operatorname{ord}_p y). \end{aligned}$$

Следовательно, $|x+y|_p = p^{-\operatorname{ord}_p(x+y)} \leqslant \max(p^{-\operatorname{ord}_p x}, p^{-\operatorname{ord}_p y}) = \max(|x|_p, |y|_p)$, а последнее $\leqslant |x|_p + |y|_p$. □

В действительности мы установили более сильное неравенство, чем требуется в условии (3), и именно это усиленное неравенство приводит нас к одному из основных понятий p-адического анализа.

Определение. Норма называется *неархимедовой*, если всегда выполнено неравенство $\|x+y\| \leqslant \max(\|x\|, \|y\|)$. Соответственно метрика называется *неархимедовой*, если $d(x, y) \leqslant \max(d(x, z), d(z, y))$; в частности, метрика, индуцированная неархимедовой нормой, неархимедова, так как в этом случае $d(x, y) = \|x-y\| = \|(x-z)+(z-y)\| \leqslant \max(\|x-z\|, \|z-y\|) = \max(d(x, z), d(z, y))$.

Таким образом, $|\ |_p$ является неархимедовой нормой на поле $\mathbb{Q}$.

Норму (или метрику), не являющуюся неархимедовой, называют *архимедовой*. Обычная абсолютная величина на поле $\mathbb{Q}$ дает пример архимедовой нормы.

Для каждого метрического пространства X определено понятие *последовательности Коши*. Последовательность $\{a_1, a_2, a_3, \ldots\}$ элементов X называется последовательностью Коши, если для всякого положительного числа ε найдется такой номер N, что $d(a_m, a_n) < \varepsilon$ при любых $m > N$ и $n > N$.

По определению, две метрики d_1 и d_2 на множестве X *эквивалентны*, если отвечающие им классы последовательностей Коши совпадают. Соответственно две нормы *эквивалентны*, если они индуцируют эквивалентные метрики.

Фиксируем вещественное число $\rho \in (0, 1)$, а затем в определении $|\ |_p$ подставим $\rho^{\operatorname{ord}_p x}$ вместо $(1/p)^{\operatorname{ord}_p x}$. Тогда мы получим неархимедову норму, эквивалентную $|\ |_p$ (см. упр. 4 и 5). Причину, по которой удобно выбирать $\rho = 1/p$, объясняет упр. 17 в конце параграфа.

Обычной абсолютной величине $|\ |$ также соответствует семейство эквивалентных ей архимедовых норм, а именно $|\ |^\alpha$, где $0 < \alpha \leqslant 1$ (см. упр. 7).

Обычную абсолютную величину мы иногда будем обозначать через $|\ |_\infty$. При этом никакой прямой связи между $|\ |_\infty$ и $|\ |_p$ не подразумевается, это всего лишь удобное обозначение.

Под «тривиальной» нормой понимается такая норма $\|\ \|$, что $\|0\| = 0$ и $\|x\| = 1$ для всех $x \neq 0$.

Теорема 1 (Островский). *Каждая нетривиальная норма $\|\ \|$ на поле $\mathbb{Q}$ эквивалентна $|\ |_p$ для некоторого простого p или $p = \infty$.*

Доказательство. Случай (i). Предположим, что существует натуральное число n, для которого $\|n\| > 1$. Пусть n_0 — наименьшее среди таких n. Так как $\|n_0\| > 1$, то $\|n_0\| = n_0^\alpha$ для некоторого положительного вещественного α. Запишем теперь произвольное целое положительное n в n_0-ичной системе:

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \ldots + a_s n_0^s,$$

где $0 \leqslant a_i < n_0$ и $a_s \neq 0$. Тогда

$$\|n\| \leqslant \|a_0\| + \|a_1 n_0\| + \|a_2 n_0^2\| + \ldots + \|a_s n_0^s\| = \\ = \|a_0\| + \|a_1\| \cdot n_0^{\alpha} + \|a_2\| \cdot n_0^{2\alpha} + \ldots + \|a_s\| \cdot n_0^{s\alpha}.$$

Так как $a_i < n_0$, то $\|a_i\| \leqslant 1$ по выбору n_0. Следовательно,

$$\|n\| \leqslant 1 + n_0^{\alpha} + n_0^{2\alpha} + \ldots + n_0^{s\alpha} = \\ = n_0^{s\alpha}(1 + n_0^{-\alpha} + \ldots + n_0^{-s\alpha}) \leqslant \\ \leqslant n^{\alpha}\left[\sum_{i=0}^{\infty} (1/n_0^{\alpha})^i\right],$$

потому что $n \geqslant n_0^s$. Выражение в квадратных скобках является константой, которую мы обозначим через C. Таким образом,

$$\|n\| \leqslant C n^{\alpha} \quad \text{для всех} \quad n = 1, 2, 3, \ldots.$$

Рассмотрим теперь достаточно большое натуральное N. Затем подставим n^N вместо n в полученное неравенство и извлечем корень степени N из обеих частей. Получим

$$\|n\| \leqslant \sqrt[N]{C}\, n^{\alpha}.$$

Переход к пределу при $N \to \infty$ и фиксированном n дает неравенство $\|n\| \leqslant n^{\alpha}$.

Обратное неравенство можно доказать следующим образом. Как и выше, представим n в n_0-ичной записи. Тогда $n_0^{s+1} > n \geqslant n_0^s$. Кроме того, поскольку $\|n_0^{s+1}\| = \|n + n_0^{s+1} - n\| \leqslant \|n\| + \|n_0^{s+1} - n\|$, то

$$\|n\| \geqslant \|n_0^{s+1}\| - \|n_0^{s+1} - n\| \geqslant n_0^{(s+1)\alpha} - (n_0^{s+1} - n)^{\alpha},$$

что следует из соотношения $\|n_0^{s+1}\| = \|n_0\|^{s+1}$ и уже установленного неравенства (т. е. $\|n\| \leqslant n^{\alpha}$) для вычитаемого члена. Значит,

$$\|n\| \geqslant n_0^{(s+1)\alpha} - (n_0^{s+1} - n_0^s)^{\alpha} = \quad (\text{так как } n \geqslant n_0^s) \\ = n_0^{(s+1)\alpha}\left[1 - \left(1 - \frac{1}{n_0}\right)^{\alpha}\right] \geqslant C' n^{\alpha}$$

для некоторой константы C', зависящей только от n_0 и α, но не от n. Затем, как и выше, подставим в

последнее неравенство n^N, извлечем корень степени N и перейдем к пределу при $N \to \infty$. В результате получаем $\|n\| \geqslant n^\alpha$.

Таким образом, $\|n\| = n^\alpha$. Далее, из свойства нормы (2) легко вывести, что $\|x\| = |x|^\alpha$ для всякого $x \in \mathbb{Q}$. Тогда из упр. 7 следует эквивалентность норм $\| \ \|$ и $| \ |$, что и заканчивает доказательство теоремы в случае (i).

Случай (ii). Предположим теперь, что $\|n\| \leqslant 1$ для всех натуральных чисел n. Пусть n_0 — наименьшее натуральное n, для которого $\|n\| < 1$. Такое n_0 существует, потому что рассматриваемая норма $\| \ \|$ нетривиальна.

Число n_0 должно быть простым. Действительно, если $n_0 = n_1 \cdot n_2$ и n_1, $n_2 < n_0$, то $\|n_1\| = \|n_2\| = 1$, а поэтому $\|n_0\| = \|n_1\| \|n_2\| = 1$. Обозначим простое число n_0 через p.

Покажем теперь, что $\|q\| = 1$ для каждого простого q, отличного от p. Предположим противное. Тогда $\|q\| < 1$ и для достаточно большого натурального N имеем $\|q^N\| = \|q\|^N < 1/2$. Аналогично, $\|p^M\| < 1/2$ для достаточно большого M. Числа p^M и q^N взаимно просты, т. е. не имеют общих делителей, отличных от 1. Поэтому можно найти (см. упр. 9) два целых числа n и m, таких, что $mp^M + nq^N = 1$. Тогда, согласно свойствам нормы (2) и (3),

$$1 = \|1\| = \|mp^M + nq^N\| \leqslant \|mp^M\| + \|nq^N\| = \\ = \|m\| \|p^M\| + \|n\| \|q^N\|.$$

Так как $\|m\|, \|n\| \leqslant 1$, то

$$1 \leqslant [p^M\| + \|q^N\| < \frac{1}{2} + \frac{1}{2} = 1,$$

и мы пришли к противоречию. Следовательно, $\|q\| = 1$.

Теорема практически доказана, поскольку каждое положительное целое число a можно разложить на простые сомножители. Пусть $a = p_1^{b_1} p_2^{b_2} \ldots p_r^{b_r}$. Тогда $\|a\| = \|p_1\|^{b_1} \cdot \|p_2\|^{b_2} \ldots \|p_r\|^{b_r}$. В последнем произведении отличен от 1 лишь тот сомножитель $\|p_i\|$, для которого $p_i = p$ (если такой найдется), причем соответствующее b_i

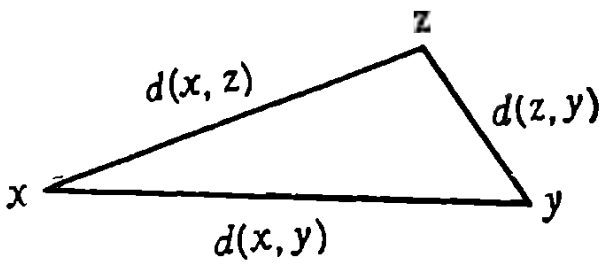
совпадает с $\operatorname{ord}_p a$. Поэтому

$$\|a\| = \rho^{\operatorname{ord}_p a},$$

где $\rho = \|p\| < 1$. На основании свойства нормы (2) легко установить, что последняя формула выполняется не только для натуральных a, но также для любого отличного от нуля рационального числа x. Из упр. 4 ниже следует эквивалентность такой нормы и нормы $|\ |_p$. Это заканчивает доказательство теоремы Островского. □

Конечно, наши интуитивные представления о расстоянии основаны на примере архимедовой метрики $|\ |_\infty$. Некоторые свойства неархимедовых метрик $|\ |_p$ поначалу кажутся довольно странными, и к ним нужно привыкать. Рассмотрим следующие два примера.

Свойство метрики (3): $d(x, y) \leqslant d(x, z) + d(z, y)$ — известно как «неравенство треугольника», поскольку в случае поля комплексных чисел $\mathbb{C}$ (с метрикой $d(a + bi, c + di) = \sqrt{(a-c)^2 + (b-d)^2}$) оно означает, что сумма длин двух сторон треугольника на комплексной плоскости больше длины третьей стороны.



Посмотрим, что происходит в случае поля F с неархимедовой нормой. Для простоты положим $z = 0$. Тогда неархимедово неравенство треугольника утверждает, что $\|x - y\| \leqslant \max(\|x\|, \|y\|)$. Предположим сначала, что «стороны» x и y имеют разную «длину», например $\|x\| < \|y\|$. Третья сторона $x - y$ имеет длину $\|x - y\| \leqslant \|y\|$. Но

$$\|y\| = \|x - (x - y)\| \leqslant \max(\|x\|, \|x - y\|),$$

и, значит, $\|y\| \leqslant \|x - y\|$, так как неравенство $\|y\| \leqslant \|x\|$ не выполнено. Поэтому $\|y\| = \|x - y\|$. Итак, если две

«стороны» x и y не равны, то наибольшая из них должна совпадать по длине с третьей стороной. Все «треугольники» равнобедренные!

Это не слишком удивительно, если понять, что означает подобное свойство для поля $\mathbb{Q}$ с нормой $|\ |_p$. Оно просто утверждает, что кратность вхождения p в разность двух рациональных чисел с неодинаковыми кратностями вхождения p совпадает с *наименьшей* из этих кратностей (это и значит равняться *наибольшей* из двух «сторон»).

Итак, для неархимедова поля $\|x \pm y\| \leqslant \max(\|x\|, \|y\|)$ и при $\|x\| \neq \|y\|$ достигается равенство. Это важное свойство впредь мы будем называть «принципом равнобедренного треугольника».

В качестве второго примера рассмотрим (открытый) диск радиуса r (r — положительное вещественное число) с центром в a (a — некоторый элемент поля F):

$$D(a, r^-) = \{x \in F \mid \|x - a\| < r\}.$$

Предположим, что норма $\|\ \|$ неархимедова. Пусть b — *произвольный* элемент $D(a, r^-)$. Тогда

$$D(a, r^-) = D(b, r^-),$$

т. е. каждая точка диска является его центром! Действительно,

$$\begin{aligned} x \in D(a, r^-) &\Rightarrow \|x - a\| < r \Rightarrow \\ &\Rightarrow \|x - b\| = \|(x - a) + (a - b)\| \leqslant \\ &\qquad \leqslant \max(\|x - a\|, \|a - b\|) < r \Rightarrow \\ &\Rightarrow x \in D(b, r^-), \end{aligned}$$

и точно так же доказывается обратная импликация.

Определим замкнутый диск радиуса r с центром в a как

$$D(a, r) = \{x \in F \mid \|x - a\| \leqslant r\};$$

тогда, как и выше, можно установить, что в случае неархимедовой нормы $\|\ \|$ каждая точка диска $D(a, r)$ является его центром.

Упражнения

1. Для произвольной нормы $\|\ \|$ на поле F докажите непрерывность операций сложения, умножения и нахождения обратного элемента относительно сложения и умножения, т. е. установите, что: (1) для любых $x, y \in F$ и любого $\varepsilon > 0$ существует такое $\delta > 0$, что $\|(x'+y')-(x+y)\| < \varepsilon$ при $\|x'-x\| < \delta$ и $\|y'-y\| < \delta$; (2) то же с заменой $\|(x'+y')-(x+y)\|$ на $\|x'y'-xy\|$; (3) для любого ненулевого $x \in F$ и любого $\varepsilon > 0$ существует такое $\delta > 0$, что $\|(1/x')-(1/x)\| < \varepsilon$ при $\|x'-x\| < \delta$; (4) для любого $x \in F$ и любого $\varepsilon > 0$ существует такое $\delta > 0$, что $\|(-x')-(-x)\| < \varepsilon$ при $\|x'-x\| < \delta$.

2. Докажите, что $\|-1\| = \|1\| = 1$ для произвольной нормы $\|\ \|$ на поле F. Докажите, что если $\|\ \|$ неархимедова, то $\|n\| \leqslant 1$ для любого целого n. (Здесь «n» обозначает $1+1+1+\ldots+1$ — результат n-кратного сложения $1 \in F$ при $n \geqslant 0$ и результат $(-n)$-кратного сложения $-1 \in F$ при $n < 0$.)

3. Докажите обратное: если норма $\|\ \|$ такова, что $\|n\| \leqslant 1$ для любого целого n, то эта норма неархимедова. (*Указание.* Рассмотрите тождество $\|x+y\|^N = \|(x+y)^N\|$. Затем, используя бином Ньютона и свойство нормы (3), оцените $\|x+y\|^N$ сверху через $\max(\|x\|, \|y\|)$. При этом нужно помнить, что N можно выбрать сколь угодно большим.)

4. Пусть $\|\ \|_1$ и $\|\ \|_2$ — две нормы на поле F. Докажите, что $\|\ \|_1 \sim \|\ \|_2$ тогда и только тогда, когда существует такое положительное вещественное число α, что $\|x\|_1 = \|x\|_2^{\alpha}$ для всех $x \in F$.

5. Докажите, что если $0 < \rho < 1$, то функция, определенная для $x \in \mathbb{Q}$ как $\rho^{\operatorname{ord}_p x}$ при $x \neq 0$ и 0 при $x = 0$, является неархимедовой нормой. Отметим, что по предыдущему упражнению эта норма эквивалентна $|\ |_p$. Что произойдет при $\rho = 1$? А при $\rho > 1$?

6. Докажите неэквивалентность норм $|\ |_{p_1}$ и $|\ |_{p_2}$ для различных простых чисел p_1 и p_2.

7. Для фиксированного вещественного $\alpha > 0$ и $x \in \mathbb{Q}$ положим $\|x\| = |x|^{\alpha}$, где $|\ |$ — обычная абсолютная величина. Докажите, что $\|\ \|$ является нормой тогда и только тогда, когда $\alpha \leqslant 1$, и что в этом случае она эквивалентна норме $|\ |$.

8. Докажите, что две эквивалентные нормы на поле F либо обе архимедовы, либо обе неархимедовы.

9. Пусть N и M — два взаимно простых целых числа. Докажите, что существуют целые n и m, для которых $nN + mM = 1$. (*Указание.* Покажите, что наименьшее положительное число вида $nN + mM$ должно быть общим делителем N и M.)

10. Вычислите:

(i) $\mathrm{ord}_3 54$, (ii) $\mathrm{ord}_2 128$, (iii) $\mathrm{ord}_3 57$,
(iv) $\mathrm{ord}_7 (-700/197)$, (v) $\mathrm{ord}_2 (128/7)$, (vi) $\mathrm{ord}_3 (7/9)$,
(vii) $\mathrm{ord}_5 (0{,}0625)$, (viii) $\mathrm{ord}_3 (10^9)$, (ix) $\mathrm{ord}_3 (-13{,}23)$,
(x) $\mathrm{ord}_7 (-13{,}23)$, (xi) $\mathrm{ord}_5 (-13{,}23)$, (xii) $\mathrm{ord}_{11} (-13{,}23)$,
(xiii) $\mathrm{ord}_{13} (-26/169)$, (xiv) $\mathrm{ord}_{103} (-1/309)$, (xv) $\mathrm{ord}_3 (91)$.

11. Докажите, что $\mathrm{ord}_p ((p^N)!) = 1 + p + p^2 + \ldots + p^{N-1}$.

12. Пусть $0 \leqslant a \leqslant p-1$. Докажите, что $\mathrm{ord}_p ((ap^N)!) = a(1 + p + p^2 + \ldots + p^{N-1})$.

13. Пусть $n = a_0 + a_1 p + a_2 p^2 + \ldots + a_s p^s$ есть p-ичное разложение натурального числа n, где $0 \leqslant a_i \leqslant p-1$. Положим $S_n = \sum a_i$ (сумма коэффициентов p-ичного разложения). Докажите, что

$$\mathrm{ord}_p (n!) = \frac{n - S_n}{p-1}.$$

14. Вычислите $|a-b|$, т. е. p-адическое расстояние от a до b, где:

(i) $a=1$, $b=26$, $p=5$; (ii) $a=1$, $b=26$, $p=\infty$;
(iii) $a=1$, $b=26$, $p=3$; (iv) $a=1/9$, $b=-1/16$, $p=5$;
(v) $a=1$, $b=244$, $p=3$; (vi) $a=1$, $b=1/244$, $p=3$;
(vii) $a=1$, $b=1/243$, $p=3$; (viii) $a=1$, $b=183$, $p=13$;
(ix) $a=1$, $b=183$, $p=7$; (x) $a=1$, $b=183$, $p=2$;
(xi) $a=1$, $b=183$, $p=\infty$; (xii) $a=91$, $b=0$, $p=3$;
(xiii) $a=(91)^2/3^9$, $b=0$, $p=3$; (xiv) $a=2^{2^N}/2^N$, $b=0$, $p=2$;
(xv) $a=2^{2^N}/(2^N)!$, $b=0$, $p=2$.

15. Объясните словами, в чем смысл неравенства $|x|_p \leqslant 1$ для рационального числа x?

16. Пусть $x \in \mathbb{Q}$. Докажите, что $\lim\limits_{i \to \infty} |x^i/i!|_p = 0$ тогда и только тогда, когда $\mathrm{ord}_p x \geqslant 1$ для $p \neq 2$ и $\mathrm{ord}_2 x \geqslant 2$.

17. Пусть x — ненулевое рациональное число. Докажите, что произведение чисел $|x|_p$ по *всем* простым p и $p=\infty$ равно 1: $\prod\limits_p |x|_p = 1$. (Отметим, что у этого «бесконечного произведения» в действительности лишь конечное число сомножителей, отличных от 1.)

18. Пусть p — простое число. Докажите, что каждая последовательность целых чисел содержит подпоследовательность Коши относительно нормы $|\ |_p$.

19. Пусть $x \in \mathbb{Q}$ и $|x|_p \leqslant 1$ для всех простых p. Докажите, что $x \in \mathbb{Z}$.

§ 3. КАК СТРОИТСЯ ПОЛЕ КОМПЛЕКСНЫХ ЧИСЕЛ

Теперь у нас есть новое понятие расстояния между рациональными числами: два рациональных числа в такой метрике тем ближе, чем на большую степень некоторого фиксированного простого p делится их разность. Чтобы работать с такими «p-адическими метриками», нам придется увеличить поле рациональных чисел $\mathbb{Q}$, подобно тому как в случае классической архимедовой метрики $|\ |$ оно пополняется до поля вещественных чисел $\mathbb{R}$ и затем расширяется до поля комплексных чисел $\mathbb{C}$. Поэтому прежде всего вспомним, как это делается.

Начнем с еще более ранней ступени, которая логически и исторически предшествовала определению поля $\mathbb{Q}$. Будем исходить из множества натуральных чисел $\mathbb{N}=\{1, 2, 3, \ldots\}$. Каждый шаг на пути от $\mathbb{N}$ к $\mathbb{C}$ можно мотивировать желанием делать без каких-либо ограничений следующие две операции:

(1) решать полиномиальные уравнения;

(2) находить пределы последовательностей Коши, т. е. так «заполнить пробелы» в числовой системе, чтобы в новой числовой системе каждая последовательность Коши имела предел.

Прежде всего на этом пути можно ввести множество всех целых чисел $\mathbb{Z}$ (включающее 0, —1, —2, ...) как множество решений уравнений вида

$$a+x=b, \quad a,\ b \in \mathbb{N}.$$

После этого можно определить рациональные числа как решения уравнений вида

$$ax=b, \quad a,\ b \in \mathbb{Z}.$$

Пока что метрика не использовалась.

Один из возможных способов точного определения вещественных чисел заключается в рассмотрении множества S, состоящего из последовательностей Коши рациональных чисел. Назовем две последовательности $s_1=\{a_j\} \in S$ и $s_2=\{b_j\} \in S$ эквивалентными и будем писать $s_1 \sim s_2$, если $|a_j-b_j| \to 0$ при $j \to \infty$. Очевидно,

$\sim$ есть отношение эквивалентности, так как: (1) каждая последовательность s эквивалентна сама себе; (2) если $s_1 \sim s_2$, то $s_2 \sim s_1$; (3) если $s_1 \sim s_2$ и $s_2 \sim s_3$, то $s_1 \sim s_3$. Определим теперь $\mathbb{R}$ как множество *классов эквивалентности* последовательностей Коши рациональных чисел. На этом множестве нетрудно определить операции сложения, умножения и нахождения обратного относительно сложения и умножения, а затем показать, что $\mathbb{R}$ является полем. Хотя на первый взгляд это определение кажется громоздким и чересчур абстрактным, тем не менее оно приводит в точности к старинному образу вещественной числовой прямой, которая допускает простое наглядное представление.

Нечто подобное произойдет, когда мы станем работать с $|\ |_p$ вместо $|\ |$. Начав с абстрактного определения p-адического пополнения поля $\mathbb{Q}$, мы придем к числовой системе с очень прозрачной структурой, которую обозначим $\mathbb{Q}_p$.

Вернемся к нашему историческому экскурсу, где мы добрались до $\mathbb{R}$. Обратившись снова к первому методу расширения числовой системы — добавлению корней уравнений, математики сочли, что неплохо иметь в запасе числа, которые позволяли бы решать такие уравнения, как $x^2+1=0$. (Здесь мы излагаем логический ход событий; исторически введение комплексных чисел предшествовало строгому определению вещественных чисел в терминах последовательностей Коши.) Тут произошло нечто удивительное! Как только было введено число $i=\sqrt{-1}$ и определено поле комплексных чисел вида $a+bi$, $a, b \in \mathbb{R}$, оказалось, что:

(1) *все* полиномиальные уравнения с коэффициентами в $\mathbb{C}$ разрешимы в $\mathbb{C}$ — это знаменитая основная теорема алгебры (короче можно сказать так: поле $\mathbb{C}$ *алгебраически замкнуто*);

(2) поле $\mathbb{C}$ полно относительно (единственной) нормы, продолжающей норму $|\ |$ с $\mathbb{R}$ (эта норма задается формулой $|a+bi|=\sqrt{a^2+b^2}$), т. е. каждая последовательность Коши $\{a_j+b_ji\}$ имеет предел вида $a+bi$ (так как $\{a_j\}$ и $\{b_j\}$ — также последовательности Коши в $\mathbb{R}$, то в качестве a и b берутся их пределы).

Итак, в данном случае процесс оканчивается на $\mathbb{C}$, которое есть всего лишь «квадратичное расширение» поля $\mathbb{R}$ (т. е. оно получается присоединением корня квадратного уравнения $x^2+1=0$). *Поле $\mathbb{C}$ алгебраически замкнуто и полно относительно архимедовой метрики.*

Но увы! В случае нормы $|\ |_p$ все не так просто. Построив $\mathbb{Q}_p$, пополнение $\mathbb{Q}$ относительно $|\ |_p$, нам придется затем образовать бесконечную последовательность расширений, задаваемых присоединением корней уравнений старших степеней (не только квадратных). Хуже того, построенное в результате алгебраически замкнутое поле, которое обозначается через $\bar{\mathbb{Q}}_p$, *не полно*. Поэтому нужно будет «заткнуть дыры» в этом и так уже громадном поле, что приведет к еще большему полю Ω.

А что потом? Не придется ли еще увеличивать Ω, для того чтобы стали разрешимы все полиномиальные уравнения с коэффициентами в Ω? Не будет ли этот процесс продолжаться все дальше и дальше, как развертывающаяся спираль все более искусственных абстракций? К счастью, тут вмешивается ангел-хранитель p-адического анализа, и уже поле Ω оказывается алгебраически замкнутым и полным. На этом наш поиск неархимедова аналога поля $\mathbb{C}$ заканчивается.

Но это поле Ω, удобная числовая система, на которой можно было бы изучать p-адический вариант классического анализа, к сожалению, понято гораздо хуже, чем $\mathbb{C}$. Как заметил И. М. Гельфанд, даже некоторые из простейших вопросов, например описание всех $\mathbb{Q}_p$-линейных автоморфизмов поля Ω, остаются пока открытыми.

Итак, начнем наше путешествие к Ω.

§ 4. ПОЛЕ p-АДИЧЕСКИХ ЧИСЕЛ

До конца этой главы p обозначает фиксированное простое число.

Пусть S — множество таких последовательностей $\{a_i\}$ рациональных чисел, что при любом $\varepsilon>0$ существует такое N, что $|a_i-a_{i'}|_p<\varepsilon$ при $i,\ i'>N$. Две такие последовательности $\{a_i\}$ и $\{b_i\}$, называемые после-

довательностями Коши, считаются эквивалентными, если $|a_i - b_i|_p \to 0$ при $i \to \infty$. Множество $\mathbb{Q}_p$, по определению, есть множество классов эквивалентности этих последовательностей Коши.

Пусть $x \in \mathbb{Q}$. Обозначим через $\{x\}$ «постоянную» последовательность Коши, все члены которой равны x. Очевидно, $\{x\} \sim \{x'\}$ тогда и только тогда, когда $x = x'$. Класс $\{0\}$ обозначим просто через 0.

Определим норму $|\ |_p$ класса эквивалентности a как предел $\lim\limits_{i\to\infty} |a_i|_p$, где $\{a_i\}$ — некоторый представитель класса a. Этот предел существует, так как:

(1) если $a = 0$, то $\lim\limits_{i\to\infty} |a_i|_p = 0$ по определению;

(2) если $a \neq 0$, то для некоторого $\varepsilon > 0$ и любого N существует $i_N > N$ с $|a_{i_N}|_p > \varepsilon$.

Действительно, если N выбрано настолько большим, что $|a_i - a_{i'}|_p < \varepsilon$ при $i,\ i' > N$, то

$$|a_i - a_{i_N}|_p < \varepsilon \quad \text{для всех } i > N.$$

Так как $|a_{i_N}|_p > \varepsilon$, то $|a_i|_p = |a_{i_N}|_p$ по принципу равнобедренного треугольника. Поэтому $|a_i|_p$ имеет постоянное значение $|a_{i_N}|_p$ при всех $i > N$. А тогда предел $\lim\limits_{i\to\infty} |a_i|_p$ равен этому постоянному значению.

Следует отметить одно существенное отличие рассматриваемого сейчас процесса пополнения от пополнения $\mathbb{Q}$ до $\mathbb{R}$. Когда мы переходим от $\mathbb{Q}$ к $\mathbb{R}$, область возможных значений функции $|\ | = |\ |_\infty$ увеличивается до множества всех неотрицательных вещественных чисел. С другой стороны, при переходе от $\mathbb{Q}$ к $\mathbb{Q}_p$ множество возможных значений $|\ |_p$, а именно $\{p^n\}_{n\in\mathbb{Z}} \cup \{0\}$, остается одним и тем же.

Пусть a и b — два класса эквивалентности рассматриваемых последовательностей Коши, а $\{a_i\} \in a$ и $\{b_i\} \in b$ — их произвольные представители. Определим $a \cdot b$ как класс эквивалентности последовательности Коши $\{a_i b_i\}$. Если $\{a_i'\} \in a$, $\{b_i'\} \in b$ — другие представители, то

$$|a_i'b_i' - a_ib_i|_p = |a_i'(b_i' - b_i) + b_i(a_i' - a_i)|_p \leqslant$$
$$\leqslant \max(|a_i'(b_i' - b_i)|_p,\ |b_i(a_i' - a_i)|_p).$$

Первое выражение в последней строке при $i \to \infty$ стремится к $|a|_p \cdot \lim |b_i' - b_i|_p = 0$, а второе — к $|b|_p \times \lim |a_i' - a_i|_p = 0$. Следовательно, $\{a_i'b_i'\} \sim \{a_ib_i\}$.

Подобным же образом можно определить сумму двух классов эквивалентности последовательностей Коши, выбрав по последовательности в каждом из этих классов, сложив их почленно, а затем показав, что класс суммы зависит только от классов слагаемых. Аналогично определяется обратный класс относительно сложения.

Определяя обратный класс относительно умножения, нужно соблюдать осторожность, ибо в последовательности Коши могут встретиться нулевые члены. Однако легко увидеть, что каждая последовательность Коши эквивалентна некоторой последовательности Коши без нулевых членов (заменим, например, все $a_i = 0$ на $a_i' = p^i$). Рассмотрим после этого последовательность $\{1/a_i\}$. Она будет последовательностью Коши, за исключением случая $|a_i|_p \to 0$, т. е. $\{a_i\} \sim \{0\}$. Более того, если $\{a_i\} \sim \{a_i'\}$ и среди a_i, a_i' нет нулей, то, как легко доказать, $\{1/a_i\} \sim \{1/a_i'\}$.

После этого нетрудно установить, что множество $\mathbb{Q}_p$ классов эквивалентности последовательностей Коши вместе с введенными на нем операциями сложения, умножения и нахождения обратных элементов является полем. Проверим, например, дистрибутивность. Пусть $\{a_i\}$, $\{b_i\}$, $\{c_i\}$ — представители классов a, b, $c \in \mathbb{Q}_p$. Тогда $a(b+c)$ есть класс эквивалентности последовательности

$$\{a_i(b_i + c_i)\} = \{a_ib_i + a_ic_i\},$$

но $ab + ac$ также совпадает с классом эквивалентности этой последовательности.

Поле $\mathbb{Q}$ можно отождествить с *подполем* в $\mathbb{Q}_p$, которое состоит из классов, содержащих постоянные последовательности Коши.

И, наконец, легко доказать полноту поля $\mathbb{Q}_p$. Действительно, пусть $\{a_j\}_{j=1, 2, \ldots}$ — последовательность классов эквивалентности, являющаяся последовательностью Коши в $\mathbb{Q}_p$. Выберем в каждом члене a_j этой последовательности по представителю, т. е. по последовательности Коши рациональных чисел $\{a_{ji}\}_{i=1, 2, \ldots}$. Тогда,

как легко показать, предел последовательности a_j равен классу эквивалентности последовательности $\{a_{jj}\}_{j=1,2,\ldots}$. Проведение доказательства мы оставляем читателю.

Вероятно, в каждом курсе или семинаре полезно проделать один раз все хлопотные проверки такого рода, чтобы не забыть полностью об аксиоматическом основании, на котором покоится все остальное. В этом частном случае абстрактный подход позволяет, кроме того, сравнить p-адическую конструкцию с конструкцией вещественных чисел и убедиться в логическом совпадении этих процедур. Однако после доказательства следующей теоремы благоразумно как можно быстрее забыть все, что связано с классами эквивалентности последовательностей Коши, и начать мыслить более конкретными понятиями.

Теорема 2. *Каждый класс эквивалентности a из $\mathbb{Q}_p$ с $|a|_p \leqslant 1$ содержит ровно одну последовательность Коши целых чисел $\{a_i\}$, для которой:*

(1) $0 \leqslant a_i < p^i$ *при* $i = 1, 2, 3, \ldots$;

(2) $a_i \equiv a_{i+1} \pmod{p^i}$ *при* $i = 1, 2, 3, \ldots$.

Доказательство. Докажем прежде всего единственность. Если $\{a_i'\}$ — другая последовательность, удовлетворяющая (1) и (2), то $a_{i_0} \neq a_{i_0}'$ для некоторого i_0. Отсюда $a_{i_0} \not\equiv a_{i_0}' \pmod{p^{i_0}}$, так как оба эти числа расположены между 0 и p^{i_0}. Но тогда для каждого $i \geqslant i_0$ имеем $a_i \equiv a_{i_0} \not\equiv a_{i_0}' \equiv a_i' \pmod{p^{i_0}}$, т. е. $a_i \not\equiv a_i' \pmod{p^{i_0}}$. Следовательно,

$$|a_i - a_i'|_p > 1/p^{i_0}$$

для всех $i \geqslant i_0$ и $\{a_i\} \not\sim \{a_i'\}$.

Теперь предположим, что задана некоторая последовательность Коши $\{b_i\} \in a$ и мы хотим найти эквивалентную ей последовательность $\{a_i\}$, удовлетворяющую (1) и (2). Используем для этого одну простую лемму.

Лемма. *Пусть $x \in \mathbb{Q}$ и $|x|_p \leqslant 1$. Тогда для любого натурального i существует целое $\alpha \in \mathbb{Z}$, для которого $|\alpha - x|_p \leqslant p^{-i}$. Более того, такое α можно выбрать из множества $\{0, 1, 2, 3, \ldots, p^i - 1\}$.*

Доказательство леммы. Пусть $x = a/b$ — несократимая дробь. Тогда p не делит b, так как $|x|_p \leqslant 1$. Следовательно, b и p^i взаимно просты. Поэтому можно найти два целых числа m и n, для которых $mb + np^i = 1$. Положим $\alpha = am$. Идея дальнейшего вычисления заключается в том, что число mb отличается от 1 на p-адически малую величину и, значит, m хорошо приближает $1/b$, а потому am хорошо приближает $x = a/b$. Точнее, имеет место оценка

$$|\alpha - x|_p = |am - (a/b)|_p = |a/b|_p\,|mb - 1|_p \leqslant$$
$$\leqslant |mb - 1|_p = |np^i|_p = |n|_p/p^i \leqslant 1/p^i.$$

Наконец, для того чтобы число α принадлежало указанному в лемме интервалу целых чисел между 0 и p^i, достаточно добавить к нему подходящее кратное p^i; при этом неравенство $|\alpha - x|_p \leqslant p^{-i}$ сохранится. Лемма доказана. □

Вернемся к доказательству теоремы. Пусть $\{b_i\}$ — наша последовательность Коши. Сопоставим каждому $j = 1, 2, 3, \ldots$ такое натуральное число $N(j)$, что $|b_i - b_{i'}|_p \leqslant p^{-j}$ при любых i, $i' \geqslant N(j)$. (Мы можем считать, что последовательность чисел $N(j)$ строго возрастает с увеличением j; в частности, $N(j) \geqslant j$.) Тогда $|b_i|_p \leqslant 1$ при $i \geqslant N(1)$, потому что для любого $i' \geqslant N(1)$

$$|b_i|_p \leqslant \max(|b_{i'}|_p,\ |b_i - b_{i'}|_p) \leqslant \max(|b_{i'}|_p,\ 1/p),$$

а $|b_{i'}|_p \to |a|_p \leqslant 1$ при $i' \to \infty$.

По предыдущей лемме мы можем найти теперь последовательность целых чисел a_j, для которой $0 \leqslant a_j < p^j$ и

$$|a_j - b_{N(j)}|_p \leqslant 1/p^j.$$

Утверждается, что последовательность $\{a_j\}$ удовлетворяет всем необходимым требованиям. Очевидно, для этого достаточно проверить сравнения $a_{j+1} \equiv a_j \pmod{p^j}$ и эквивалентность $\{b_i\} \sim \{a_j\}$. Первое следует из неравенств

$$|a_{j+1} - a_j| = |a_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} - (a_j - b_{N(j)})|_p \leqslant$$
$$\leqslant \max(|a_{j+1} - b_{N(j+1)}|_p,\ |b_{N(j+1)} - b_{N(j)}|_p,\ |a_j - b_{N(j)}|_p) \leqslant$$
$$\leqslant \max(1/p^{j+1},\ 1/p^j,\ 1/p^j) = 1/p^j.$$

Для доказательства второго утверждения возьмем произвольное j. Тогда для любого $i \geqslant N(j)$

$$|a_i - b_i|_p = |a_i - a_j + a_j - b_{N(j)} - (b_i - b_{N(j)})|_p \leqslant$$
$$\leqslant \max(|a_i - a_j|_p,\ |a_j - b_{N(j)}|_p,\ |b_i - b_{N(j)}|_p) \leqslant$$
$$\leqslant \max(1/p^j,\ 1/p^j,\ 1/p^i) = 1/p^j.$$

Поэтому $|a_i - b_i|_p \to 0$ при $i \to \infty$, и теорема доказана. □

Что делать, если наше p-адическое число a не удовлетворяет неравенству $|a|_p \leqslant 1$? В этом случае умножим a на подходящую степень p^m числа p (например, на степень числа p, равную $|a|_p$) так, чтобы новое p-адическое число $a' = ap^m$ уже удовлетворяло неравенству $|a'|_p \leqslant 1$. Выберем затем в соответствии с теоремой 2 последовательность $\{a'_i\}$, представляющую a'. Тогда число $a = a'p^{-m}$ представляется последовательностью $\{a_i\}$ с $a_i = a'_i p^{-m}$.

Для удобства запишем теперь все числа a'_i последовательности, соответствующей a', в p-ичной системе счисления, т. е. положим

$$a'_i = b_0 + b_1 p + b_2 p^2 + \ldots + b_{i-1} p^{i-1},$$

где коэффициенты b_j обозначают «p-ичные знаки», т. е. целые числа из множества $\{0, 1, \ldots, p-1\}$. Сравнение $a'_i \equiv a'_{i+1} \pmod{p^i}$ из теоремы 2 эквивалентно тому, что все знаки числа

$$a'_{i+1} = b_0 + b_1 p + b_2 p^2 + \ldots + b_{i-1} p^{i-1} + b_i p^i,$$

от b_0 до b_{i-1} включительно, *совпадают* с соответствующими знаками числа a'_i. Поэтому a' можно представлять себе интуитивно как число, имеющее бесконечную вправо p-ичную запись: всякий раз, переходя от a'_i к a'_{i+1}, мы добавляем в этой записи новый знак.

Теперь и наше исходное число a можно представлять себе как p-ичное число с конечным числом знаков «направо от запятой» (т. е. знаков, соответствующих отрицательным степеням p; в нашей записи они начинаются слева), но с бесконечным числом знаков при положительных степенях p:

$$a = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \ldots + \frac{b_{m-1}}{p} + b_m + b_{m+1} p + b_{m+2} p^2 + \ldots .$$

Пока что правую часть этого равенства следует понимать как сокращенную запись последовательности $\{a_i\}$, где $a_i = b_0 p^{-m} + \ldots + b_{i-1} p^{i-1-m}$, т. е. как удобный способ изображения сразу всей последовательности $\{a_i\}$. Вскоре мы убедимся, что в некотором точном смысле это равенство есть «настоящее равенство». Оно называется «p-адическим разложением» числа a.

Пусть $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leqslant 1\}$. Это множество всех чисел из $\mathbb{Q}_p$, p-адическое разложение которых не содержит отрицательных степеней p. Элементы $\mathbb{Z}_p$ называются *целыми p-адическими числами*. (Чтобы избежать путаницы, начиная с этого места обычные целые из $\mathbb{Z}$ мы называем *целыми рациональными*.) Сумма, разность и произведение двух элементов из $\mathbb{Z}_p$ снова принадлежат $\mathbb{Z}_p$. Поэтому $\mathbb{Z}_p$ — *подкольцо* поля $\mathbb{Q}_p$.

Пусть a, $b \in \mathbb{Q}_p$. Мы пишем $a \equiv b \pmod{p^n}$, если $|a-b|_p \leqslant p^{-n}$, или, эквивалентно, $(a-b)/p^n \in \mathbb{Z}_p$, т. е. если первый отличный от нуля знак в p-адическом разложении числа $a-b$ встречается не ранее, чем на p^n-м месте. В случае когда a и b лежат не только в $\mathbb{Q}_p$, но также и в $\mathbb{Z}$ (т. е. они целые рациональные), это определение согласуется с данным выше определением сравнения $a \equiv b \pmod{c}$ для $c = p^n$.

В дальнейшем через $\mathbb{Z}_p^\times$ будем обозначать множество $\{x \in \mathbb{Z}_p \mid 1/x \in \mathbb{Z}_p\}$, или, эквивалентно, $\{x \in \mathbb{Z}_p \mid x \not\equiv 0 \pmod{p}\}$, или, эквивалентно, $\{x \in \mathbb{Z}_p \mid |x|_p = 1\}$. Целые p-адические числа из $\mathbb{Z}_p^\times$, т. е. числа, имеющие ненулевой первый знак, называют иногда p-адическими единицами.

Пусть теперь $\{b_i\}_{i=-m}^{\infty}$ — произвольная последовательность целых p-адических чисел. Рассмотрим частичные суммы

$$S_N = \frac{b_{-m}}{p^m} + \frac{b_{-m+1}}{p^{m-1}} + \ldots + b_0 + b_1 p + b_2 p^2 + \ldots + b_N p^N.$$

Последовательность, состоящая из этих сумм, является последовательностью Коши: если $M > N$, то $|S_N - S_M|_p < 1/p^N$. Следовательно, она сходится к некоторому элементу из $\mathbb{Q}_p$. Как и в случае бесконечных рядов вещест-

венных чисел, определим $\sum_{i=-m}^{\infty} b_i p^i$ как предел последовательности частичных сумм в $\mathbb{Q}_p$.

Более общо, если $\{c_i\}$ — *произвольная* последовательность p-адических чисел и $|c_i|_p \to 0$ при $i \to \infty$, то последовательность частичных сумм $S_N = c_1 + c_2 + \ldots + c_N$ сходится к пределу, который обозначается через $\sum_{i=1}^{\infty} c_i$. В самом деле, $|S_M - S_N|_p = |c_{N+1} + c_{N+2} + \ldots + c_M|_p \leqslant \max(|c_{N+1}|_p, |c_{N+2}|_p, \ldots, |c_M|_p)$, а потому $\to 0$ при $N \to \infty$. Отсюда видно, что проверять сходимость бесконечных p-адических рядов проще, чем бесконечных рядов вещественных чисел. *Ряд сходится в поле $\mathbb{Q}_p$ тогда и только тогда, когда последовательность его членов стремится к нулю.* В p-адическом случае нет ничего подобного гармоническому ряду $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots$ вещественных чисел, который расходится, несмотря на то, что его члены стремятся к 0. Напомним, почему это так: норма $|\ |_p$ суммы двух чисел не превосходит *максимума* (а не суммы) норм слагаемых, если $p \neq \infty$, т. е. если норма $|\ |_p$ неархимедова.

Вернемся к p-адическим разложениям. Бесконечный ряд

$$\frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \ldots + \frac{b_{m-1}}{p} + b_m + b_{m+1}p + b_{m+2}p^2 + \ldots$$

(здесь $b_i \in \{0, 1, 2, \ldots, p-1\}$) в определении p-адического разложения сходится к a. Значит, это выражение можно истолковать содержательно как сумму бесконечного ряда.

Отметим, что утверждаемая в теореме 2 единственность не имеет места в архимедовом случае. Так, всякая конечная десятичная дробь может быть записана и в виде десятичной дроби с бесконечно повторяющейся цифрой 9 на конце, например $1 = 0{,}9999\ldots$. В противоположность этому два p-адических разложения, сходящихся к одному и тому же числу из $\mathbb{Q}_p$, совпадают, т. е. имеют все одинаковые знаки.

В заключение сделаем еще одно замечание. В качестве множества p-ичных знаков мы могли бы выбрать не только $\{0, 1, 2, \ldots, p-1\}$, но также и любое другое множество $S = \{\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{p-1}\}$ целых p-адических чисел, для которых $\alpha_i \equiv i \pmod{p}$ при $i = 0, 1, 2, \ldots, p-1$. Тогда p-адическое разложение можно определить как сумму вида $\sum_{i=-m}^{\infty} = b_i p^i$, где теперь роль «знаков» b_i играют элементы множества S, а не множества $\{0, 1, \ldots, p-1\}$. Множество $\{0, 1, \ldots, p-1\}$ подходит для почти всех надобностей. Тем не менее существует другое множество S, в некоторых отношениях более естественное. Это множество так называемых представителей Тейхмюллера (см. ниже упр. 12).

§ 5. АРИФМЕТИКА В $\mathbb{Q}_p$

Техника выполнения операций сложения, вычитания, умножения и деления p-адических чисел во многом напоминает соответствующие операции с десятичными дробями, изучаемые в начальной школе. Единственное отличие в том, что «занимание», «перенос в другой разряд», «умножение столбиком» и т. д. делаются слева направо, а не справа налево. Вот несколько примеров вычислений в $\mathbb{Q}_7$:

$$\begin{array}{r} 3+6\times7+2\times7^2+\ldots \\ \times\ 4+5\times7+1\times7^2+\ldots \\ \hline 5+4\times7+4\times7^2+\ldots \\ 1\times7+4\times7^2+\ldots \\ 3\times7^2+\ldots \\ \hline 5+5\times7+4\times7^2+\ldots \end{array} \qquad \begin{array}{r} 2\times7^{-1}+0\times7^0+3\times7^1+\ldots \\ -\ 4\times7^{-1}+6\times7^0+5\times7^1+\ldots \\ \hline 5\times7^{-1}+0\times7^0+4\times7^1+\ldots \end{array}$$

$$\begin{array}{r} 1+2\times7+4\times7^2+\ldots \\ 1+6\times7+1\times7^2+\ldots \\ \hline 3\times7+2\times7^2+\ldots \\ 3\times7+5\times7^2+\ldots \\ \hline 4\times7^2+\ldots \\ \underline{4\times7^2+\ldots} \end{array} \qquad \begin{array}{r|l} 3+5\times7+1\times7^2+\ldots & \\ \hline 5+1\times7+6\times7^2+\ldots & \end{array}$$

В качестве еще одного примера попробуем извлечь корень $\sqrt{6}$ в $\mathbb{Q}_5$. Мы хотим найти последовательность целых чисел $a_0, a_1, a_2, \ldots$, для которой $0 \leqslant a_i \leqslant 4$ и

$$(a_0 + a_1 \times 5 + a_2 \times 5^2 + \ldots)^2 = 1 + 1 \times 5.$$

Сравнивая коэффициенты при $1 = 5^0$ в обеих частях равенства, получаем $a_0^2 \equiv 1 \pmod 5$, откуда $a_0 = 1$ или 4. Возьмем $a_0 = 1$. Тогда, сравнивая коэффициенты при 5 в обеих частях, получаем $2a_1 \times 5 \equiv 1 \times 5^2 \pmod{5^2}$. Следовательно, $2a_1 \equiv 1 \pmod 5$ и $a_1 = 3$. На следующем шаге мы должны решить сравнение

$$1 + 1 \times 5 \equiv (1 + 3 \times 5 + a_2 \times 5^2)^2 \equiv$$
$$\equiv 1 + 1 \times 5 + 2a_2 \times 5^2 \pmod{5^3}.$$

Следовательно, $2a_2 \equiv 0 \pmod 5$ и $a_2 = 0$. Продолжая этот процесс далее, получаем ряд

$$a = 1 + 3 \times 5 + 0 \times 5^2 + 4 \times 5^3 + a_4 \times 5^4 + a_5 \times 5^5 + \ldots,$$

в котором каждый коэффициент a_i определяется однозначно после выбора a_0.

Напомним, однако, что при выборе a_0 мы имели две возможности, а именно 1 или 4. А если бы мы выбрали 4, а не 1? В этом случае мы получили бы

$$-a = 4 + 1 \times 5 + 4 \times 5^2 + 0 \times 5^3 +$$
$$+ (4 - a_4) \times 5^4 + (4 - a_5) \times 5^5 + \ldots.$$

Тот факт, что для a_0 имеется два возможных выбора и что, когда выбор сделан, последующие числа $a_1, a_2, a_3, \ldots$ определены однозначно, просто отражает то обстоятельство, что в таких полях, как $\mathbb{Q}$, $\mathbb{R}$ или $\mathbb{Q}_p$, если у ненулевого элемента есть хоть один квадратный корень, то их ровно два.

Всякое ли число из $\mathbb{Q}_5$ имеет квадратный корень? Мы видели, что 6 имеет. А 7? Из равенства

$$(a_0 + a_1 \times 5 + \ldots)^2 = 2 + 1 \times 5$$

следовало бы сравнение $a_0^2 \equiv 2 \pmod 5$. Но оно неразрешимо — это легко установить перебором всех значений $a_0 = 0, 1, 2, 3, 4$. Поэтому 7 не имеет квадратного корня в $\mathbb{Q}_5$. Более систематическое представление о квадратных корнях в $\mathbb{Q}_p$ можно получить из упр. 5 — 11.

Как показывает следующая важная «лемма», изложенный выше метод решения уравнения $x^2-6=0$ в $\mathbb{Q}_5$ — решение сравнения $a_0^2-6\equiv 0 \pmod 5$ и затем последовательное нахождение остальных a_i — является весьма общим.

Теорема 3 (лемма Гензеля). *Пусть* $F(x)=c_0+c_1x+\ldots+c_nx^n$ — *многочлен с целыми p-адическими коэффициентами, а* $F'(x)=c_1+2c_2x+3c_3x^2+\ldots+nc_nx^{n-1}$ — *его производная. Предположим, что* a_0 — *целое p-адическое число, для которого* $F(a_0)\equiv 0 \pmod p$, *а* $F'(a_0)\not\equiv 0 \pmod p$. *Тогда существует единственное целое p-адическое число a, такое, что*

$$F(a)=0 \text{ и } a\equiv a_0 \pmod p.$$

(*Замечание.* В нашем примере $F(x)=x^2-6$, $F'(x)=2x$, $a_0=1$.)

Доказательство леммы Гензеля. Прежде всего утверждается существование и единственность последовательности целых рациональных чисел $a_1, a_2, a_3, \ldots$, для которой при любом $n\geqslant 1$:

(1) $F(a_n)\equiv 0 \pmod{p^{n+1}}$;
(2) $a_n\equiv a_{n-1} \pmod{p^n}$;
(3) $0\leqslant a_n<p^{n+1}$.

Докажем это индукцией по n.

Пусть $n=1$. Обозначим через $\tilde{a}_0$ единственное целое число из множества $\{0, 1, \ldots, p-1\}$, сравнимое с a_0 по модулю p. Тогда всякое a_1, удовлетворяющее (2) и (3), можно представить в виде $\tilde{a}_0+b_1p$, где $0\leqslant b_1\leqslant p-1$. Рассмотрим выражение $F(\tilde{a}_0+b_1p)$ и раскроем в нем скобки, помня, что нас интересует результат только по модулю p^2, так что все члены, делящиеся на p^2, можно опускать:

$$\begin{aligned}F(a_1)=F(\tilde{a}_0+b_1p)&=\sum c_i(\tilde{a}_0+b_1p)^i=\\&=\sum\left(c_i\tilde{a}_0^i+ic_i\tilde{a}_0^{i-1}b_1p+\text{члены, делящиеся на } p^2\right)\equiv\\&\equiv\sum c_i\tilde{a}_0^i+\left(\sum ic_i\tilde{a}_0^{i-1}\right)b_1p \pmod{p^2}=\\&=F(\tilde{a}_0)+F'(\tilde{a}_0)\,b_1p.\end{aligned}$$

(Обратите внимание на сходство с формулой из анализа для приближения первого порядка функции рядом Тейлора: $F(x+h)=F(x)+F'(x)h+$ члены более высокого порядка.) По предположению, $F(a_0)\equiv 0 \pmod p$, откуда $F(\tilde a_0)\equiv \alpha p \pmod{p^2}$ для некоторого $\alpha\in\{0, 1, \ldots, p-1\}$. Поэтому сравнение $F(a_1)\equiv 0 \pmod{p^2}$ эквивалентно сравнению $\alpha p + F'(\tilde a_0) b_1 p \equiv 0 \pmod{p^2}$, или $\alpha + F'(\tilde a_0) b_1 \equiv 0 \pmod p$. Так как, по предположению, $F'(a_0)\not\equiv 0 \pmod p$, последнее сравнение разрешимо относительно неизвестного b_1. Действительно, пользуясь леммой из доказательства теоремы 2, выберем такое $b_1\in\{0, 1, \ldots, p-1\}$, что $b_1\equiv -\alpha/F'(\tilde a_0) \pmod p$. Очевидно, $b_1\in\{0, 1, \ldots, p-1\}$, удовлетворяющее данному условию, единственно.

Теперь, переходя к общему шагу индукции, предположим, что мы уже отыскали $a_1, a_2, \ldots, a_{n-1}$. Требуется найти a_n. По условиям (2) и (3) это число вида $a_n = a_{n-1} + b_n p^n$, где $b_n\in\{0, 1, \ldots, p-1\}$. Раскроем скобки и приведем выражение $F(a_{n-1}+b_n p^n)$ к подходящему виду, как и выше в случае $n=1$, только на этот раз не будем учитывать члены, делящиеся на p^{n+1}. Получим

$$F(a_n) = F(a_{n-1}+b_n p^n) \equiv F(a_{n-1}) + F'(a_{n-1}) b_n p^n \pmod{p^{n+1}}.$$

Так как по индуктивному предположению $F(a_{n-1})\equiv 0 \pmod{p^n}$, то $F(a_{n-1})\equiv \alpha' p^n \pmod{p^{n+1}}$. Нужное нам условие $F(a_n)\equiv 0 \pmod{p^{n+1}}$ принимает вид

$$\alpha' p^n + F'(a_{n-1}) b_n p^n \equiv 0 \pmod{p^{n+1}}, \quad \text{т. е.}$$
$$\alpha' + F'(a_{n-1}) b_n \equiv 0 \pmod p.$$

Из сравнения $a_{n-1}\equiv a_0 \pmod p$ легко вывести, что $F'(a_{n-1})\equiv F'(a_0)\not\equiv 0 \pmod p$. Тогда требуемое $b_n\in\{0, 1, \ldots, p-1\}$ находится точно так же, как и b_1 в рассмотренном выше случае, т. е. из сравнения $b_n\equiv -\alpha'/F'(a_{n-1}) \pmod p$. На этом индукция заканчивается, и наше утверждение доказано.

Теорема следует теперь непосредственно из этого утверждения. Действительно, возьмем $a=\tilde a_0 + b_1 p + b_2 p^2 + \ldots$. Тогда p-адическое число $F(a)$ равно 0, так как $F(a)\equiv F(a_n)\equiv 0 \pmod{p^{n+1}}$ для всех n. Обратно,

если a удовлетворяет требованиям теоремы и $a = \tilde{a}_0 + b_1 p + b_2 p^2 + \ldots$ — его p-адическое разложение, то последовательность $\{a_n\}$ удовлетворяет требованиям доказанного утверждения. Отсюда получаем единственность такой последовательности, а значит, и единственность искомого a. Лемма Гензеля доказана. □

Лемму Гензеля часто называют p-адической леммой Ньютона, потому что метод последовательного приближения, использованный в ее доказательстве, по существу

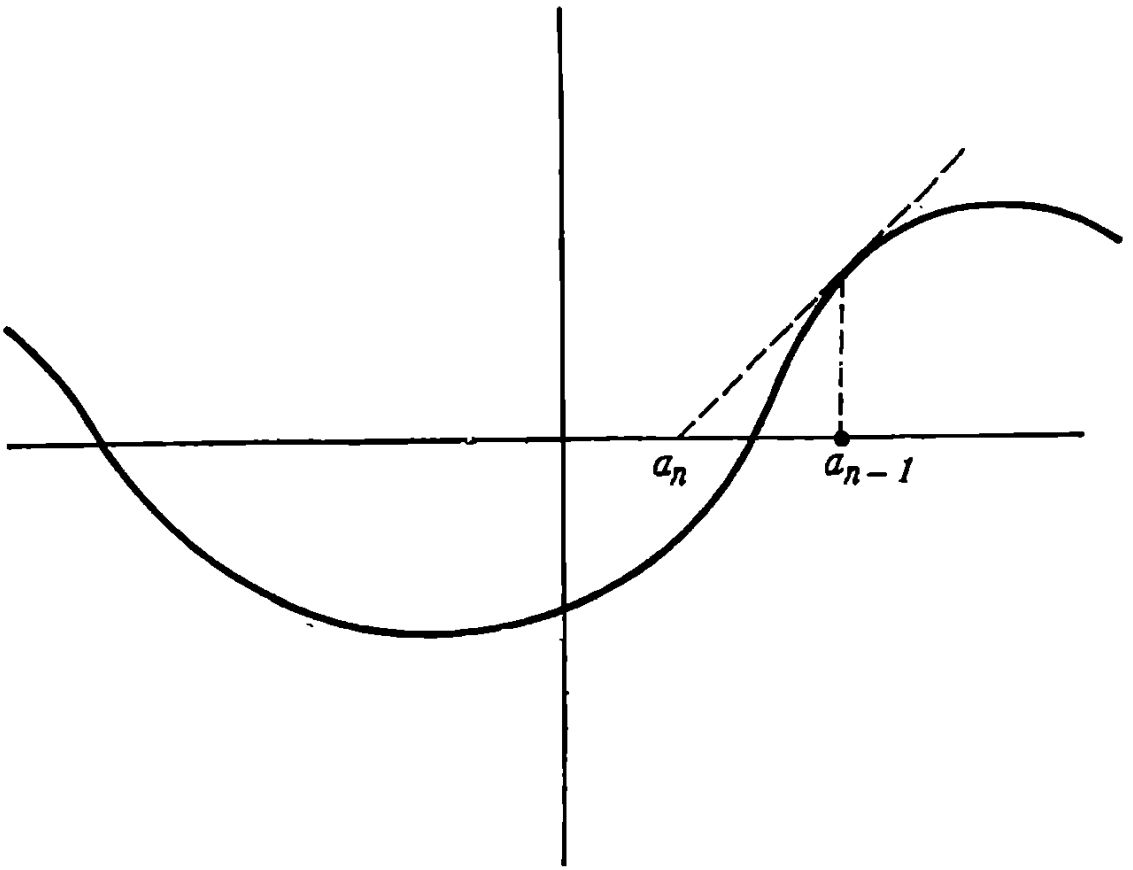


Рис. I.1. Метод Ньютона в вещественном случае.

совпадает с методом Ньютона нахождения *вещественного* корня вещественного многочлена. Если $f'(a_{n-1}) \neq 0$, то в вещественном случае по методу Ньютона в качестве следующего приближения берется

$$a_n = a_{n-1} - \frac{f(a_{n-1})}{f'(a_{n-1})}$$

(см. рис. I.1). Поправочный член $-f(a_{n-1})/f'(a_{n-1})$ в этой формуле очень похож на «поправочный член» в дока-

зательстве леммы Гензеля:

$$b_n p^n \equiv -\frac{\alpha' p^n}{F'(a_{n-1})} \equiv -\frac{F(a_{n-1})}{F'(a_{n-1})} \pmod{p^{n+1}}.$$

Но в одном отношении p-адический метод Ньютона (лемма Гензеля) лучше, чем метод Ньютона в вещественном случае. В p-адическом варианте *гарантирована* сходимость к некоторому корню многочлена. В вещественном же случае метод Ньютона *обычно* сходится,

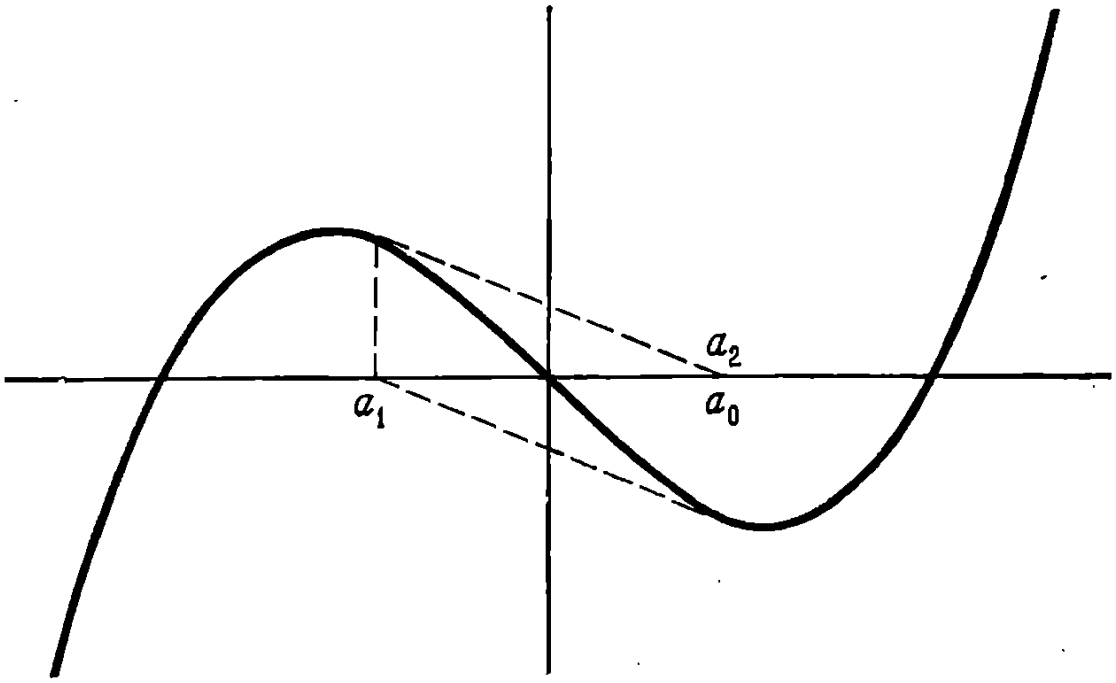


Рис. I.2. Неудачное применение метода Ньютона в вещественном случае.

но — не всегда. Например, если мы рассмотрим $f(x) = x^3 - x$ и сделаем неудачный выбор $a_0 = 1/\sqrt{5}$, то получим

$$a_1 = 1/\sqrt{5} - [1/5\sqrt{5} - 1/\sqrt{5}]/(3/5 - 1) =$$
$$= (1/\sqrt{5})[1 - (1/5 - 1)/(3/5 - 1)] = -1/\sqrt{5};$$
$$a_2 = 1/\sqrt{5}; \quad a_3 = -1/\sqrt{5}$$

и т. д. (см. рис. I.2). В $\mathbb{Q}_p$ такая несуразица невозможна.

Упражнения

1. Пусть $a \in \mathbb{Q}_p$ имеет p-адическое разложение $a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \ldots + a_0 + a_1 p \ldots$. Как выглядит p-адическое разложение $-a$?

2. Найдите p-адическое разложение для:

(i) $(6+4\times7+2\times7^2+1\times7^3+\ldots)(3+0\times7+0\times7^2+6\times7^3+\ldots)$ в $\mathbb{Q}_7$ с четырьмя знаками;

(ii) $1/(3+2\times5+3\times5^2+1\times5^3+\ldots)$ в $\mathbb{Q}_5$ с четырьмя знаками;

(iii) $9\times11^2-(3\times11^{-1}+2+1\times11^1+3\times11^2+\ldots)$ в $\mathbb{Q}_{11}$ с четырьмя знаками;

(iv) $2/3$ в $\mathbb{Q}_2$; (v) $-1/6$ в $\mathbb{Q}_7$; (vi) $1/10$ в $\mathbb{Q}_{11}$;
(vii) $-9/16$ в $\mathbb{Q}_{13}$; (viii) $1/1000$ в $\mathbb{Q}_5$; (ix) $6!$ в $\mathbb{Q}_3$;
(x) $1/3!$ в $\mathbb{Q}_3$; (xi) $1/4!$ в $\mathbb{Q}_2$; (xii) $1/5!$ в $\mathbb{Q}_5$.

3. Докажите, что p-адическое разложение числа $a\in\mathbb{Q}_p$ обрывается (т. е. $a_i=0$ для всех i, больших некоторого N) тогда и только тогда, когда a является *положительным* рациональным числом со знаменателем, равным степени p.

4. Докажите, что p-адическое разложение числа $a\in\mathbb{Q}_p$ начиная с некоторого места периодично (т. е. $a_{i+r}=a_i$ при некотором r и всех i, больших некоторого N) тогда и только тогда, когда $a\in\mathbb{Q}$.

5. Докажите следующее обобщение леммы Гензеля. Пусть $F(x)$ — многочлен с коэффициентами в $\mathbb{Z}_p$. Если для некоторого $a_0\in\mathbb{Z}_p$ мы имеем $F(a_0)\equiv0\pmod{p^{2M+1}}$, $F'(a_0)\equiv0\pmod{p^M}$, но $F'(a_0)\not\equiv0\pmod{p^{M+1}}$, то существует и притом единственное $a\in\mathbb{Z}_p$, для которого $F(a)=0$ и $a\equiv a_0\pmod{p^{M+1}}$.

6. Воспользовавшись своим доказательством упр. 5, найдите квадратный корень из -7 в $\mathbb{Q}_2$ с пятью знаками.

7. Какие из следующих 11-адических чисел имеют квадратные корни в $\mathbb{Q}_{11}$?

(i) 5; (ii) 7; (iii) -7;
(iv) $5+3\times11+9\times11^2+1\times11^3$;
(v) $3\times11^{-2}+6\times11^{-1}+3+0\times11+7\times11^2$;
(vi) $3\times11^{-1}+6+3\times11+0\times11^2+7\times11^3$;
(vii) 1×11^7; (viii) $7-6\times11^2$; (ix) $5\times11^{-2}+\sum_{n=0}^{\infty}n\times11^n$.

8. Вычислите $\pm\sqrt{-1}$ в $\mathbb{Q}_{13}$ с четырьмя знаками.

9. Для каких $p=2$, 3, 5, 7, 11, 13, 17, 19 можно извлечь квадратный корень из -1 в $\mathbb{Q}_p$?

10. Пусть p — произвольное нечетное простое число. Предположим, что $\alpha\in\mathbb{Q}_p$ и $|\alpha|_p=1$. Опишите способ узнать, существует или нет квадратный корень из α в $\mathbb{Q}_p$. Как действовать, если $|\alpha|_p\neq1$? Докажите существование такой четверки чисел α_1, α_2, α_3, $\alpha_4\in\mathbb{Q}_p$, что для любого отличного от нуля $\alpha\in\mathbb{Q}_p$ среди чисел $\alpha_1\alpha$, $\alpha_2\alpha$, $\alpha_3\alpha$, $\alpha_4\alpha$ ровно одно имеет квадратный корень в $\mathbb{Q}_p$. (Если заменить p на ∞, а $\mathbb{Q}_p$ на $\mathbb{R}$, то существуют *два* числа, например ±1, таких, что для любого ненулевого $\alpha\in\mathbb{R}$ ровно одно из чисел $1\cdot\alpha$ и $-1\cdot\alpha$ имеет квадратный корень в $\mathbb{R}$.)

11. Решите ту же задачу, что и в упр. 10, для $p=2$. В этом случае требуется найти *восемь* чисел $\alpha_1, \ldots, \alpha_8 \in \mathbb{Q}_2$, таких, что для любого ненулевого $\alpha \in \mathbb{Q}_2$ ровно одно из чисел $\alpha_1\alpha, \ldots, \alpha_8\alpha$ имеет квадратный корень в $\mathbb{Q}_2$. (Конечно, выбор такой восьмерки $\alpha_1, \ldots, \alpha_8$ *не однозначен*.)

12. Найдите первые четыре знака p-адических разложений всех четырех корней степени 4 из 1 в $\mathbb{Q}_5$. Докажите, что уравнение $x^p - x = 0$ всегда имеет p решений $a_0, a_1, \ldots a_{p-1}$ в $\mathbb{Q}_p$, для которых $a_i \equiv i \pmod p$. Эти p чисел называются представителями Тейхмюллера для $\{0, 1, 2, \ldots, p-1\}$ и используются иногда в качестве p-ичных знаков вместо $\{0, 1, 2, \ldots, p-1\}$.

13. Докажите следующий «признак неприводимости Эйзенштейна». Пусть $f(x) = a_0 + a_1x + \ldots + a_nx^n$ — многочлен с коэффициентами $a_i \in \mathbb{Z}_p$. Если $a_i \equiv 0 \pmod p$ при $i = 0, 1, 2, \ldots, n-1$, $a_n \not\equiv 0 \pmod p$ и $a_0 \not\equiv 0 \pmod{p^2}$, то $f(x)$ неприводим над $\mathbb{Q}_p$, т. е. не представим в виде произведения двух многочленов меньшей степени с коэффициентами в $\mathbb{Q}_p$.

14. Используя упр. 13, покажите, что 1 не имеет других корней степени p, кроме 1, в $\mathbb{Q}_p$ при $p > 2$. (*Указание*: подставьте $y = x - 1$ в $(x^p - 1)/(x - 1)$.) Докажите это также другим способом: представьте любой такой корень x в виде $1 + p^r x'$, где $|x'|_p = 1$, а $r > 0$ — некоторое целое (объясните, почему $x \equiv 1 \pmod p$), затем это выражение для x возведите в степень p, раскройте скобки и сравните коэффициенты при степенях p.

15. Докажите, что ряд $1 + p + p^2 + p^3 + \ldots$ сходится к $1/(1-p)$ в $\mathbb{Q}_p$. К чему сходятся $1 - p + p^2 - p^3 + p^4 - p^5 + \ldots$ и $1 + (p-1)p + p^2 + (p-1)p^3 + p^4 + (p-1)p^5 + \ldots$?

16. Предположим, что n — целое (положительное или отрицательное) число, не делящееся на p, и $\alpha \equiv 1 \pmod p$. Покажите, что α имеет корень степени n в $\mathbb{Q}_p$. Приведите пример, показывающий, что при $p = n$ это неверно. Покажите, что α имеет корень степени p, если $\alpha \equiv 1 \pmod{p^2}$ и $p \neq 2$.

17. Пусть $\alpha \in \mathbb{Z}_p$. Докажите сравнения $\alpha^{p^M} \equiv \alpha^{p^{M-1}} \pmod{p^M}$ для $M = 1, 2, 3, 4, \ldots$. Докажите, что последовательность $\{\alpha^{p^M}\}$ стремится к некоторому пределу в $\mathbb{Q}_p$ и что этот предел равен представителю Тейхмюллера, сравнимому с α по модулю p.

18. Докажите, что $\mathbb{Z}_p$ секвенциально компактно, т. е. что каждая последовательность целых p-адических чисел содержит сходящуюся подпоследовательность.

19. Рассмотрим матрицы с элементами в $\mathbb{Q}_p$. Суммы, произведения и определители этих матриц задаются точно так же, как и в вещественном случае. Пусть $M = \{r \times r$-матрицы с элементами в $\mathbb{Z}_p\}$, $M^\times = \{A \in M \mid A$ обратима в $M\}$ (легко видеть, что это равносильно условию $\det A \in \mathbb{Z}_p^\times$), и пусть $pM = \{A \in M \mid A = pB$, где $B \in M\}$. Докажите, что если $A \in M^\times$ и $B \in pM$, то существует единственная матрица $X \in M^\times$, для которой $X^2 - AX + B = 0$.

Глава II

p-АДИЧЕСКАЯ ИНТЕРПОЛЯЦИЯ ДЗЕТА-ФУНКЦИИ РИМАНА

Эта глава логически не связана с последующими и помещена здесь как плато (по уровню абстракции) на середине нашего восхождения к Ω. Все происходящее в этой главе еще не выходит за рамки полей $\mathbb{Q}$, $\mathbb{Q}_p$ и $\mathbb{R}$.

Дзета-функция Римана ζ определяется на множестве вещественных чисел >1 формулой

$$\zeta(s) \underset{\text{def}}{=} \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Легко установить (сравнивая с интегралом $\int_1^{\infty} (dx/x^s) = 1/(s-1)$ при фиксированном $s>1$) сходимость этой суммы при $s>1$.

Пусть p — произвольное простое число. Цель этой главы заключается в доказательстве некоторой «p-адической непрерывности» последовательности чисел $\zeta(2k)$ для $k=1, 2, 3, \ldots$. Точнее, пусть $2k$ пробегает все четные положительные целые числа из фиксированного класса вычетов по модулю $p-1$. Сопоставим каждому из них значение

$$f(2k) = (1 - p^{2k-1}) \frac{c_k}{\pi^{2k}} \zeta(2k),$$

где $c_k = (-1)^k (2k-1)!/2^{2k-1}$. Оказывается, число $f(2k)$ всегда рационально. Кроме того, если два числа вида $2k$ из рассматриваемого класса вычетов p-адически близки (т. е. их разность делится на большую степень p), то, как мы увидим в дальнейшем, соответствующие им

значения $f(2k)$ также p-адически близки. (При этом нам понадобится еще одно предположение: $2k$ не делится на $p-1$.) По существу это означает, что функцию f можно однозначно продолжить до *непрерывной функции f, определенной на множестве целых p-адических чисел и принимающей значения в $\mathbb{Q}_p$*. (Непрерывность понимается здесь, как в классическом анализе: если $\{x_n\}$ p-адически сходится к x, то $\{f(x_n)\}$ p-адически сходится к $f(x)$.)

Эту процедуру мы называем *p-адической интерполяцией*. Она аналогична классическому методу, скажем, определения функции $f(x)=a^x$ (где a — фиксированное вещественное положительное число): сначала определяем значения $f(x)$ для рациональных x, затем доказываем близость значений a^x при близких рациональных x и в заключение определяем a^x для иррационального x как предел a^{x_n} по рациональным x_n, стремящимся к x.

Отметим, что любую функцию f на множестве S, например, четных положительных чисел можно продолжить до непрерывной функции на $\mathbb{Z}_p$ не более чем одним способом (при $p\neq 2$). Это следует из *плотности* подмножества S в $\mathbb{Z}_p$: любое $x\in\mathbb{Z}_p$ представимо в виде предела последовательности целых четных положительных чисел x_n. Действительно, если f — непрерывная функция, то $f(x)=\lim\limits_{n\to\infty} f(x_n)$. В вещественном же случае множество рациональных чисел плотно в $\mathbb{R}$, а S — нет. Поэтому условие непрерывности не определяет еще вещественную интерполяцию функции, заданной на множестве четных положительных чисел. Таких интерполяций всегда бесконечно много. (Однако при некоторых дополнительных требованиях на вещественную интерполирующую функцию, помимо непрерывности, она может оказаться единственной. Например, гамма-функция $\Gamma(x+1)$ интерполирует $k!$ для целых неотрицательных $x=k$. Кроме того, она удовлетворяет функциональному уравнению $\Gamma(x+1)=x\Gamma(x)$ при всех вещественных x, а ее логарифм является выпуклой функцией при $x>0$. Этими условиями гамма-функция характеризуется однозначно.)

§ 1. ФОРМУЛА ДЛЯ ЗНАЧЕНИЙ $\zeta(2k)$

Рассмотрим следующее разложение Тейлора:

$$\frac{t}{e^t-1}=\frac{1}{1+t/2!+t^2/3!+t^3/4!+\ldots+t^n/(n+1)!+\ldots}=$$
$$\overset{\text{def}}{=}\sum_{k=0}^{\infty}B_k t^k/k!.$$

Произведение k-го коэффициента этого степенного ряда на $k!$ называется k-м числом Бернулли и обозначается через B_k. Вот несколько первых B_k:

$$B_0=1,\quad B_1=-1/2,\quad B_2=1/6,\quad B_3=0,$$
$$B_4=-1/30,\quad B_5=0,\quad B_6=1/42,\ \ldots.$$

В этом параграфе мы установим формулу

$$\zeta(2k)=(-1)^k\pi^{2k}\frac{2^{2k-1}}{(2k-1)!}\left(-\frac{B_{2k}}{2k}\right)\quad\text{для}\quad k=1,\ 2,\ 3,\ \ldots.$$

Напомним определение гиперболического синуса, обозначаемого через sh:

$$\operatorname{sh}x=\frac{e^x-e^{-x}}{2}.$$

Для него мы имеем следующее разложение Тейлора:

$$\operatorname{sh}x=x+\frac{x^3}{3!}+\frac{x^5}{5!}+\ldots+\frac{x^{2k+1}}{(2k+1)!}+\ldots,$$

которое получается усреднением соответствующих рядов для e^x и $-e^{-x}$. Отметим, что он отличается от ряда Тейлора для $\sin x$ отсутствием чередования знаков.

Предложение. *Бесконечное произведение*

$$\pi x\prod_{n=1}^{\infty}\left(1+\frac{x^2}{n^2}\right)$$

сходится при любом вещественном x и равно $\operatorname{sh}(\pi x)$.

Доказательство. Сходимость следует непосредственно из логарифмического признака:

$$\sum_{n=1}^{\infty}\left|\log\left(1+\frac{x^2}{n^2}\right)\right|\leqslant\sum_{n=1}^{\infty}\frac{x^2}{n^2}<\infty\quad\text{при любом } x.$$

Доказательству равенства мы предпошлем вывод разложения в бесконечное произведение для $\sin x$.

Лемма. *Пусть $n=2k+1$ — целое нечетное положительное число. Тогда существуют многочлены P_n и Q_{n-1} с целыми коэффициентами степени, не превосходящей n и $n-1$ соответственно, такие, что*

$$\sin(nx)=P_n(\sin x),\quad \cos(nx)=\cos x\,Q_{n-1}(\sin x).$$

Доказательство леммы. Воспользуемся индукцией по k. Для $k=0$ (т. е. $n=1$) лемма очевидна. Предположим, что она уже доказана для $k-1$. Тогда

$$\begin{aligned}\sin[(2k+1)x]&=\sin[(2k-1)x+2x]=\\&=\sin(2k-1)x\cos 2x+\cos(2k-1)x\sin 2x=\\&=P_{2k-1}(\sin x)(1-2\sin^2 x)+\\&\qquad+\cos x Q_{2k-2}(\sin x)\,2\sin x\cos x,\end{aligned}$$

откуда легко получить нужное представление вида $P_{2k+1}(\sin x)$. Проверка соответствующего утверждения для $\cos(2k+1)x$ аналогична, и мы оставляем ее читателю. □

Продолжим теперь доказательство предложения. Прежде всего, подставив $x=0$ в тождество $\sin nx=P_n(\sin x)$, мы устанавливаем, что постоянный член у P_n равен нулю. Затем, продифференцировав $\sin nx=P_n(\sin x)$ по x, получим

$$n\cos nx=P_n'(\sin x)\cos x.$$

Подставим в это тождество $x=0$; мы увидим, что $n=P_n'(0)$, т. е. первый коэффициент многочлена P_n равен n. Следовательно,

$$\frac{\sin nx}{n\sin x}=\tilde{P}_{2k}(\sin x)=1+a_1\sin x+a_2\sin^2 x+\ldots$$
$$\ldots+a_{2k}\sin^{2k}x\quad(n=2k+1),$$

где a_i — некоторые рациональные числа. Отметим теперь, что левая часть обращается в нуль при $x=\pm\pi/n,\ldots$ $\ldots,\pm k\pi/n$. Кроме того, все $2k$ значений $y=\pm\sin\pi/n$, $\pm\sin 2\pi/n,\ldots,\sin k\pi/n$, в которых обращается в нуль многочлен $\tilde{P}_{2k}(y)$, различны; степень $\tilde{P}_{2k}$ равна $2k$,

а постоянный член равен 1. Поэтому

$$\tilde{P}_{2k}(y)=\left(1-\frac{y}{\sin \pi/n}\right)\left(1-\frac{y}{-\sin \pi/n}\right)\left(1-\frac{y}{\sin 2\pi/n}\right)\times$$
$$\times\left(1-\frac{y}{-\sin 2\pi/n}\right)\ldots\left(1-\frac{y}{\sin k\pi/n}\right)\left(1-\frac{y}{-\sin k\pi/n}\right)=$$
$$=\prod_{r=1}^{k}\left(1-\frac{y^2}{\sin^2 r\pi/n}\right).$$

Следовательно,

$$\frac{\sin nx}{n\sin x}=\tilde{P}_{2k}(\sin x)=\prod_{r=1}^{k}\left(1-\frac{\sin^2 x}{\sin^2 r\pi/n}\right).$$

Подставив $\pi x/n$ вместо x, получаем

$$\frac{\sin \pi x}{n\sin \pi x/n}=\prod_{r=1}^{k}\left(1-\frac{\sin^2 \pi x/n}{\sin^2 r\pi/n}\right).$$

Перейдем теперь к пределу при $n=2k+1\to\infty$ в обеих частях последнего тождества. Левая часть стремится к $(\sin \pi x)/\pi x$. При r, достаточно малом по сравнению с n, r-й член произведения близок к $1-((\pi x/n)/(\pi r/n))^2=1-x^2/r^2$. Отсюда следует, что произведение сходится к $\prod_{r=1}^{\infty}(1-x^2/r^2)$. (Строгую проверку мы оставляем читателю в качестве одного из приведенных ниже упражнений.)

Таким образом,

$$\prod_{n=1}^{\infty}\left(1-\frac{x^2}{n^2}\right)=\frac{\sin \pi x}{\pi x}=1-\frac{\pi^2x^2}{3!}+\frac{\pi^4x^4}{5!}-\frac{\pi^6x^6}{7!}+\frac{\pi^8x^8}{9!}-\ldots.$$

Правая часть — это разложение синуса в ряд Тейлора. С другой стороны,

$$\frac{\operatorname{sh} \pi x}{\pi x}=1+\frac{\pi^2x^2}{3!}+\frac{\pi^4x^4}{5!}+\frac{\pi^6x^6}{7!}+\frac{\pi^8x^8}{9!}+\ldots.$$

Если мы раскроем скобки в бесконечном произведении для $\sin(\pi x)/\pi x$, то знак минус будет только у тех членов, которые содержат нечетное число сомножителей вида x^2/n^2, т. е. в точности у тех членов, которые подобны членам со знаком минус в ряде Тейлора для $\sin(\pi x)/\pi x$. Следовательно, изменение знака внутри сомножителей полученного разложения вызовет изменение в ряде справа всех минусов на плюсы, что и доказывает требуемое равенство. (Для «лучшего» понимания этого завершающего шага см. упр. 3.) □

Теперь мы готовы доказать обещанную выше формулу.

Теорема 4.

$$\zeta(2k) = (-1)^k \pi^{2k} \frac{2^{2k-1}}{(2k-1)!}\left(-\frac{B_{2k}}{2k}\right).$$

Доказательство. Прологарифмируем обе части тождества

$$\operatorname{sh} \pi x = \pi x \prod_{n=1}^{\infty}\left(1+\frac{x^2}{n^2}\right)$$

(при $x>0$). Слева мы получим

$$\log \operatorname{sh} \pi x = \log[(e^{\pi x}-e^{-\pi x})/2] = \log[(e^{\pi x}/2)(1-e^{-2\pi x})] =$$
$$= \log(1-e^{-2\pi x}) + \pi x - \log 2.$$

Справа, пользуясь разложением Тейлора функции $\log(1+x)$, получим

$$\log \pi + \log x + \sum_{n=1}^{\infty} \log(1+x^2/n^2) =$$
$$= \log \pi + \log x + \sum_{n=1}^{\infty}\sum_{k=1}^{\infty} (-1)^{k+1}\frac{x^{2k}}{kn^{2k}}.$$

Последний двойной ряд сходится абсолютно при $0<x<1$. Поэтому можно изменить в нем порядок суммиро-

вания и получить тождество

$$\log(1-e^{-2\pi x})+\pi x-\log 2=$$
$$=\log\pi+\log x+\sum_{k=1}^{\infty}\left[(-1)^{k+1}\frac{x^{2k}}{k}\sum_{n=1}^{\infty}\frac{1}{n^{2k}}\right]=$$
$$=\log\pi+\log x+\sum_{k=1}^{\infty}(-1)^{k+1}\frac{x^{2k}}{k}\zeta(2k).$$

Продифференцируем теперь обе части этого тождества по x. Ряд справа можно дифференцировать почленно, так как ряд из производных сходится равномерно на каждом интервале $0<x<1-\varepsilon$ при $\varepsilon>0$. Следовательно,

$$\frac{2\pi e^{-2\pi x}}{1-e^{-2\pi x}}+\pi=\frac{1}{x}+2\sum_{k=1}^{\infty}(-1)^{k+1}x^{2k-1}\zeta(2k).$$

Умножив на x, а затем подставив $x/2$ вместо x, получим

$$\frac{\pi x}{e^{\pi x}-1}+\frac{\pi x}{2}=1+\sum_{k=1}^{\infty}\frac{(-1)^{k+1}\zeta(2k)}{2^{2k-1}}x^{2k}.$$

Левая часть разлагается в ряд $\pi x/2+\sum\limits_{k=0}^{\infty}B_k(\pi x)^k/k!$. Сравнивая коэффициенты при четных степенях x, получаем равенство $\pi^{2k}B_{2k}/(2k)!=((-1)^{k+1}/2^{2k-1})\zeta(2k)$, что и завершает доказательство теоремы. □

Вот несколько примеров:

$$\zeta(2)=\frac{\pi^2}{6},\quad \zeta(4)=\frac{\pi^4}{90},\quad \zeta(6)=\frac{\pi^6}{945}.$$

Формула для $\zeta(2k)$ из теоремы 4 предусмотрительно записана в таком виде, в котором выделены «интересная» часть $-B_{2k}/2k$ и нежелательный множитель $(-1)^k\pi^{2k}\times$ $\times 2^{2k-1}/(2k-1)!$. Именно эту интересную часть мы и будем p-адически интерполировать. Позднее (в § 7) мы представим некоторые мотивы для выделения $-B_{2k}/2k$

«из общего котла». Пока отметим лишь, что от π^{2k} обязательно следует избавиться при p-адической интерполяции значений дзета-функции, поскольку нет разумной p-адической интерпретации вещественных трансцендентных чисел. (Как определить, например, их p-адический порядок?)

§ 2. p-АДИЧЕСКАЯ ИНТЕРПОЛЯЦИЯ ФУНКЦИИ $f(s)=a^s$

Этот параграф сыграет свою роль в дальнейшем изложении. Сюда же он помещен в учебных целях: как на макете, мы ознакомимся с некоторыми чертами p-адической интерполяции, которые могли бы иначе вызвать недоумение.

Пусть a — некоторое фиксированное положительное вещественное число. Мы уже отмечали выше, что функцию $f(s)=a^s$ можно определить как непрерывную функцию вещественного аргумента, задав ее сначала на множестве рациональных чисел, а затем «интерполируя» или «продолжая по непрерывности» на все вещественные числа, каждое из которых представимо в виде предела последовательности рациональных чисел.

Предположим теперь, что $a=n$ — некоторое фиксированное целое положительное число. Будем рассматривать n как элемент $\mathbb{Q}_p$. Тогда для каждого целого неотрицательного s целое число n^s принадлежит $\mathbb{Z}_p$. Множество всех целых неотрицательных чисел плотно в $\mathbb{Z}_p$, как и множество $\mathbb{Q}$ в $\mathbb{R}$. Действительно, каждое целое p-адическое число представимо как предел последовательности целых неотрицательных чисел (например, последовательности частичных сумм его p-адического разложения). Поэтому функцию $f(s)=n^s$ можно попытаться продолжить по непрерывности с множества целых неотрицательных s на все целые p-адические s.

Для этого необходимо выяснить, близки ли два значения n^s и $n^{s'}$ для близких целых положительных s и s', например для $s'=s+p^N$ при достаточно большом N. Как показывают следующие два примера, это верно не всегда:

(1) $n=p$, $s=0$; тогда $|n^s-n^{s'}|_p=|1-p^{p^N}|_p=1$ независимо от N;

(2) $1<n<p$; тогда по малой теореме Ферма (см. первый абзац в доказательстве теоремы 9 из § III.1) $n \equiv n^p \pmod p$, поэтому $n \equiv n^p \equiv n^{p^2} \equiv n^{p^3} \equiv \ldots \ldots \equiv n^{p^N} \pmod p$; отсюда $n^s - n^{s+p^N} = n^s(1-n^{p^N}) \equiv n^s(1-n) \pmod p$, а значит, $|n^s - n^{s'}|_p = 1$ независимо от N.

Но наше положение не столь безнадежно, как может показаться после двух таких примеров. Рассмотрим такое n, что $n \equiv 1 \pmod p$, т. е. $n = 1 + mp$. Пусть $|s'-s|_p \leqslant 1/p^N$, иными словами, $s' = s + s''p^N$ для некоторого $s'' \in \mathbb{Z}$. Тогда (если, скажем, $s' > s$)

$$|n^s - n^{s'}|_p = |n^s|_p\,|1 - n^{s'-s}|_p = |1 - n^{s'-s}|_p = \\ = |1 - (1+mp)^{s''p^N}|_p.$$

Но из разложения

$$(1+mp)^{s''p^N} = 1 + (s''p^N)\,mp + \frac{s''p^N(s''p^N-1)}{2}(mp)^2 + \ldots \\ \ldots + (mp)^{s''p^N}$$

видно, что слагаемые в $1-(1+mp)^{s''p^N}$ делятся на p^{N+1}. Следовательно,

$$|n^s - n^{s'}|_p \leqslant |p^{N+1}|_p = \frac{1}{p^{N+1}}.$$

Иначе говоря, если $s'-s$ делится на p^N, то $n^s - n^{s'}$ делится на p^{N+1}.

Итак, если $n \equiv 1 \pmod p$, то мы можем определить значение функции $f(s) = n^s$ для *любого целого p-адического* s как целое p-адическое число, равное пределу значений n^{s_i} по любой последовательности целых неотрицательных чисел s_i, стремящейся к s (например, по последовательности частичных сумм p-адического разложения s). Тогда $f(s)$ — непрерывная функция на $\mathbb{Z}_p$ со значениями в $\mathbb{Z}_p$.

Можно добиться чуть большего и определить n^s для любого n, не делящегося на p. С этой целью потребуем, кроме сравнимости чисел s и s' по модулю большой степени p, их сравнимости по модулю $p-1$. Точнее, фиксируем некоторое $s_0 \in \{0, 1, 2, 3, \ldots, p-2\}$ и вместо того, чтобы рассматривать значения n^s для всех

целых неотрицательных s, рассмотрим значения n^s только для s, сравнимых с фиксированным s_0 по модулю $p-1$. Пусть $s = s_0 + (p-1)s_1$, где s_1 — произвольное неотрицательное целое число. Тогда выделенные значения приводят к числам $n^{s_0+(p-1)s_1}$. После этого мы можем провести p-адическую интерполяцию, так как

$$n^s = n^{s_0}(n^{p-1})^{s_1}$$

и $n^{p-1} \equiv 1 \pmod{p}$ для любого n, не делящегося на p. Действительно, здесь n^{p-1} играет ту же роль, что и n в предыдущем абзаце, а s_1 — роль s (*постоянный множитель* n^{s_0} несуществен).

В результате мы получили интерполирующую функцию f, которую можно ввести еще так. Пусть S_{s_0} — множество целых неотрицательных чисел, сравнимых с s_0 по модулю $p-1$. Множество S_{s_0} плотно в $\mathbb{Z}_p$ (см. ниже упр. 7). Тогда функцию $f\colon S_{s_0} \to \mathbb{Z}_p$, заданную формулой $f(s) = n^s$, можно однозначно продолжить по непрерывности до функции $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$. Заметим, что так определенная функция f зависит от s_0, а не только от n.

В случае когда $n \equiv 0 \pmod{p}$, мы сталкиваемся с действительной трудностью. Это происходит потому, что $n^{s_i} \to 0$ p-адически для *любой* возрастающей последовательности целых неотрицательных чисел. В самом деле, любая последовательность целых неотрицательных чисел, стремящихся к числу $s \in \mathbb{Z}_p$, которое не является целым неотрицательным числом, содержит бесконечно возрастающую подпоследовательность. Поэтому единственным кандидатом на роль интерполирующей функции в этом случае будет нулевая функция, что нелепо.

В заключение отметим, что предыдущие рассуждения дословно переносятся на случай функции $1/n^s$ (см. ниже упр. 8).

Вернемся снова к дзета-функции Римана

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (s > 1).$$

Можно попытаться наивно проинтерполировать каждый член ряда $\zeta(s)$ и затем сложить результаты. Но из

этого ничего не выйдет, потому что уже сумма одних только поддающихся интерполяции членов, для которых $p \nmid n$, расходится в $\mathbb{Z}_p$. Тем не менее давайте временно забудем про это и рассмотрим ряд почленно.

Прежде всего желательно избавиться от всех членов $1/n^s$, для которых n делится на p. Сделаем это следующим образом:

$$\zeta(s) = \sum_{n=1,\ p\nmid n}^{\infty} \frac{1}{n^s} + \sum_{n=1,\ p\mid n}^{\infty} \frac{1}{n^s} =$$

$$= \sum_{n=1,\ p\nmid n}^{\infty} \frac{1}{n^s} + \sum_{n=1}^{\infty} \frac{1}{p^s n^s} = \sum_{n=1,\ p\nmid n}^{\infty} \frac{1}{n^s} + \frac{1}{p^s}\zeta(s);$$

$$\zeta(s) = \frac{1}{1-1/p^s} \sum_{n=1,\ p\nmid n}^{\infty} \frac{1}{n^s}.$$

В дальнейшем мы будем работать именно с этой последней суммой

$$\zeta^*(s) \underset{\text{def}}{=} \sum_{n=1,\ p\nmid n}^{\infty} \frac{1}{n^s} = \left(1-\frac{1}{p^s}\right)\zeta(s).$$

Эта процедура известна как *выделение эйлерова p-множителя*. Название связано со знаменитой формулой

$$\zeta(s) = \prod_{\text{простые } q} \frac{1}{1-1/q^s}$$

(см. ниже упр. 1). Множитель $1/(1-1/q^s)$ в этом произведении, соответствующий простому числу q, называется *эйлеровым q-множителем*. Таким образом, умножая $\zeta(s)$ на $(1-1/p^s)$, мы уничтожаем эйлеров p-множитель и получаем

$$\zeta^*(s) = \prod_{\text{простые } q\neq p} \frac{1}{1-1/q^s}.$$

Теперь мы намерены выбрать $s_0 \in \{0, 1, 2, \ldots, p-2\}$ и ограничить область изменения аргумента до множества всех $s \in S_{s_0} = \{s,\ s \equiv s_0 \pmod{p-1}\}$.

В дальнейшем окажется, что введенные в § 1 числа $-B_{2k}/2k$ после умножения на $1-p^{2k-1}$ могут быть проинтерполированы для $2k \in S_{2s_0}$ ($2s_0 \in \{0, 2, 4, \ldots, p-3\}$). Отметим здесь, что умножение происходит не на $[1-(1/p^{2k})]$, как можно было бы ожидать, а на эйлеров множитель с аргументом $1-2k$ вместо $2k$: $1-(1/p^{1-2k}) = 1-p^{2k-1}$. Причина довольно естественной замены $2k \leftrightarrow 1-2k$ будет объяснена в § 7. (Мы увидим, что «интересующий нас множитель» $-B_{2k}/2k$ в $\zeta(2k)$ равен в действительности $\zeta(1-2k)$; значения $\zeta(x)$ и $\zeta(1-x)$ связаны между собой некоторым «функциональным уравнением».)

Точнее, мы установим следующий факт: если $2k$, $2k' \in S_{2k_0}$ (где $2k_0 \in \{2, 4, \ldots, p-3\}$; в случае $k_0 = 0$ формулировка немного сложнее) и $k \equiv k' \pmod{p^N}$, то (см. § 6)

$$(1-p^{2k-1})(-B_{2k}/2k) \equiv (1-p^{2k'-1})(-B_{2k'}/2k') \pmod{p^{N+1}}.$$

Эти сравнения впервые были открыты Куммером около ста лет назад. Но их интерпретация в связи с p-адической интерполяцией ζ-функции Римана была получена только в 1964 г. Куботой и Леопольдтом.

Упражнения

1. Докажите, что для $s > 1$

$$\zeta(s) = \prod_{\text{простые } q} \frac{1}{1-q^{-s}}.$$

2. Докажите, что при $n = 2k+1 \to \infty$

$$\prod_{r=1}^{k} \frac{1-\sin^2(\pi x/n)/\sin^2(\pi r/n)}{1-x^2/r^2} \to 1.$$

3. Используя формулу $e^{ix} = \cos x + i \sin x$, покажите, что $\operatorname{sh} x = -i \sin ix$. Затем другим способом выведите бесконечное произведение для $\operatorname{sh} x$ из произведения для $\sin x$.

4. Докажнте, что $B_k = 0$ для нечетных $k > 1$.

5. Используя формулу для $\zeta(2k)$ в сочетании с асимптотической формулой Стирлинга $n! \sim \sqrt{2\pi n}\, n^n e^{-n}$ (где знак $\sim$ означает, что отношение обеих частей стремится к 1 при $n \to \infty$), вычислите асимптотику обычной архимедовой абсолютной величины для B_{2k}.

6. Вычислите с четырьмя знаками p-адическую фуикцию из § 2 в следующих случаях:

(i) $11^{1/601}$ в $\mathbb{Q}_5$; (ii) $\sqrt{1/10}$ в $\mathbb{Q}_3$;

(iii) $(-6)^{2+4\cdot7+3\cdot7^2+7^3+\dots}$ в $\mathbb{Q}_7$.

7. Пусть $s_0 \in \{0, 1, \dots, p-2\}$. Докажите, что множество целых неотрицательных чисел, сравнимых с s_0 по модулю $p-1$, плотно в $\mathbb{Z}_p$, т. е. каждое число из $\mathbb{Z}_p$ приближается этими числами с любой степенью точности.

8. Что произойдет, если в рассуждениях § 2 целое положительное число n заменить на $n \in \mathbb{Z}_p$? А если вместо функции $f(s)=n^s$ рассмотреть $f(s)=1/n^s$? Заметим, что последнее эквивалентно выбору в качестве плотного подмножества в $\mathbb{Z}_p$ множества *неположительных целых чисел* вместо *неотрицательных* при той же интерполируемой функции f.

9. Рассмотрим фуикцию χ, заданную на множестве целых положительных чисел следующим образом:

$$\chi(n)=\begin{cases} 1, & \text{если } n\equiv 1 \pmod 4;\\ -1, & \text{если } n\equiv 3 \pmod 4;\\ 0, & \text{если } 2 \mid n.\end{cases}$$

Положим $L_\chi(s) \overset{\text{def}}{=} \sum_{n=1}^{\infty} (\chi(n)/n^s) = 1-(1/3^s)+(1/5^s)-(1/7^s)+\dots$.

Докажите, что $L_\chi(s)$ сходится при $s>0$, а при $s>1$ сходится абсолютно. Найдите $L_\chi(1)$. Найдите также эйлеровы произведения для $L_\chi(s)$ и $L^*_\chi(s) \overset{\text{def}}{=} \sum_{n\geqslant 1,\ p\nmid n} (\chi(n)/n^s)$. (Оказывается, для значений $L_\chi(2k+1)$ (т. е. здесь для *нечетных* аргументов вместо четных) существует формула, аналогичная формуле теоремы 4: число

$$B_{\chi,n} \overset{\text{def}}{=} n! \cdot \left(\text{коэффициент при } t^n \text{ в } \frac{te^t}{e^{4t}-1}-\frac{te^{3t}}{e^{4t}-1}\left(=\frac{-t}{e^t+e^{-t}}\right)\right)$$

заменяет B_n.)

Замечание. Упражнение 9 относится к частному случаю следующей ситуации. Пусть N — целое положительное число, а $(\mathbb{Z}/N\mathbb{Z})^\times$ — мультипликативная группа классов вычегов по модулю N целых чисел, взаимно простых с N. Пусть χ: $(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ — гомоморфизм группы $(\mathbb{Z}/N\mathbb{Z})^\times$ в мультипликативную группу ненулевых элементов поля комплексных чисел. (Легко установить, что образу χ в $\mathbb{C}$ принадлежат только корни из 1.) Гомоморфизм χ называется *характером* группы $(\mathbb{Z}/N\mathbb{Z})^\times$. Предположим, что χ — *примитивный* характер, т. е. не существует целого M, делящего N, для которого $1 \leqslant M < N$ и значения χ на элементах из $(\mathbb{Z}/N\mathbb{Z})^\times$ зависят только от их класса по модулю M. Обозначим через χ также функцию на множестве всех целых чисел n, равную $\chi(n \bmod N)$ для n, взаимно простых с N, и 0 в остальных случаях. Такая функция χ называется *характером Дирихле с кондуктором* N.

Определим теперь

$$L_\chi(s) \overset{\text{def}}{=} \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Для этой функции можно найти явную формулу, подобную формуле из теоремы 4: число

$$B_{\chi,n} \overset{\text{def}}{=} n! \cdot \left(\text{коэффициент при } t^n \text{ в } \sum_{a=1}^{N-1} \frac{\chi(a)\, te^{at}}{e^{Nt}-1} \right)$$

заменит B_n. Эта формула задает значения L_χ для четных целых, если $\chi(-1)=1$, и для нечетных, если $\chi(-1)=-1$. (См. книгу Ивасавы [(c) 1].)

Кроме того, имеет место явная формула

$$L_\chi(1) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} =$$

$$= \begin{cases} -\dfrac{\tau(\chi)}{N} \displaystyle\sum_{a=1}^{N-1} \bar{\chi}(a) \log \sin \frac{a\pi}{N}, & \text{если} \quad \chi(-1)=1; \\ \dfrac{\pi i \tau(\chi)}{N^2} \displaystyle\sum_{a=1}^{N-1} \bar{\chi}(a) \cdot a, & \text{если} \quad \chi(-1)=-1, \end{cases}$$

где черта над χ обозначает комплексное сопряжение характера: $\bar{\chi}(a) \overset{\text{def}}{=} \overline{\chi(a)}$, а числа

$$\tau(\chi) \overset{\text{def}}{=} \sum_{a=1}^{N-1} \chi(a)\, e^{2\pi i a/N}$$

известны как гауссовы суммы. (Доказательство этого факта можно найти, например, в книге Боревича и Шафаревича [(b) 1], стр. 442—444.)

10. Используя предыдущую формулу для $L_\chi(1)$, проверьте полученное вами значение $L_\chi(1)$ в упр. 9. Докажите также, что:

(a) $\dfrac{1}{1} - \dfrac{1}{2} + \dfrac{1}{4} - \dfrac{1}{5} + \dfrac{1}{7} - \dfrac{1}{8} + \dfrac{1}{10} - \dfrac{1}{11} + \ldots + \dfrac{1}{3k+1} - \dfrac{1}{3k+2} + \ldots = \dfrac{\pi}{3\sqrt{3}}$;

(b) $\dfrac{1}{1} - \dfrac{1}{3} - \dfrac{1}{5} + \dfrac{1}{7} + \dfrac{1}{9} - \dfrac{1}{11} - \dfrac{1}{13} + \dfrac{1}{15} + \dfrac{1}{17} - \dfrac{1}{19} - \dfrac{1}{21} + \dfrac{1}{23} + \ldots = \dfrac{\log(1+\sqrt{2})}{\sqrt{2}}$.

§ 3. *p*-АДИЧЕСКИЕ РАСПРЕДЕЛЕНИЯ

В качестве «базиса открытых множеств» метрического пространства $\mathbb{Q}_p$ можно взять систему множеств $a + p^N\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x-a|_p \leqslant 1/p^N\}$, где $a \in \mathbb{Q}_p$, а $N \in \mathbb{Z}$. Это означает, что любое открытое подмножество в $\mathbb{Q}_p$ представимо в виде объединения открытых множеств такого вида. Множества $a + p^N\mathbb{Z}_p$ в этой главе называются *интервалами* (в других местах мы часто будем называть их *дисками*) и обозначаются также через $a + (p^N)$. Отметим, что все интервалы одновременно открыты и замкнуты. Они замкнуты, так как дополнение к $a + (p^N)$ равно объединению открытых множеств $a' + (p^N)$ по всем $a' \in \mathbb{Q}_p$, для которых $a' \notin a + (p^N)$.

Напомним, что пространство $\mathbb{Z}_p$ секвенциально компактно, т. е. каждая последовательность целых p-адических чисел содержит сходящуюся подпоследовательность (см. упр. 18 к § I.5). Очевидно, то же самое справедливо для любого интервала или их конечного объединения. Для любого метрического пространства X секвенциальная компактность некоторого подмножества $S \subset X$ эквивалентна следующему свойству, называемому просто *компактностью*: если S содержится в объединении открытых множеств, то оно содержится в некотором объединении конечного числа этих множеств (*каждое открытое покрытие обладает конечным подпокрытием*). (См. Симмонс [(а) 1], § 24; эта книга является хорошей сводкой понятий из общей топологии [1]).) Отсюда следует, что открытое подмножество в $\mathbb{Q}_p$ компактно тогда и только тогда, когда оно есть объединение конечного числа интервалов (см. ниже упр. 1). Такие подмножества, называемые «компактно-открытыми», все время появляются в этом параграфе.

Определение. Пусть X и Y — два топологических пространства. Отображение $f\colon X \to Y$ называется *локально постоянным*, если каждая точка $x \in X$ обладает такой окрестностью U, что $f(U)$ — одноэлементное подмножество Y.

---

[1]) См. также Куратовский [(а) 6], т. 1, § 41. — *Прим. перев.*

Очевидно, любая локально постоянная функция непрерывна.

В классическом анализе понятие локально постоянной функции малоупотребительно, потому что обычно все такие функции постоянны. Последнее верно для всякого связного X, например для $\mathbb{R}$ и $\mathbb{C}$.

Но у нас X будет компактно-открытым подмножеством в $\mathbb{Q}_p$ (как правило, $\mathbb{Z}_p$ или $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid |x|_p = 1\}$). На таких пространствах существует много нетривиальных локально постоянных функций. Точнее, $f\colon X \to \mathbb{Q}_p$ локально постоянна тогда и только тогда, когда f представима в виде конечной линейной комбинации характеристических функций компактно-открытых подмножеств (см. ниже упр. 4).

Локально постоянные функции играют для p-адических подпространств X ту же роль, что ступенчатые функции при определении интеграла Римана в случае $X = \mathbb{R}$.

Пусть теперь X — компактно-открытое подпространство в $\mathbb{Q}_p$, такое, как $\mathbb{Z}_p$ или $\mathbb{Z}_p^\times$.

Определение. Линейный над $\mathbb{Q}_p$ гомоморфизм μ $\mathbb{Q}_p$-векторного пространства локально постоянных функций на X в $\mathbb{Q}_p$ называется *p-адическим распределением на* X. Пусть $f\colon X \to \mathbb{Q}_p$ — некоторая локально постоянная функция. Вместо $\mu(f)$ мы обычно пишем $\int f\mu$.

Эквивалентное определение (см. ниже упр. 4). Аддитивное отображение μ множества компактно-открытых подмножеств в X со значениями в $\mathbb{Q}_p$ называется *p-адическим распределением на* X. Аддитивность означает, что для всякого разбиения множества $U \subset X$ на компактно-открытые подмножества $U_1, U_2, \ldots, U_n$

$$\mu(U) = \mu(U_1) + \mu(U_2) + \ldots + \mu(U_n).$$

Эквивалентность определений означает, что всякое μ во втором смысле однозначно «продолжается» до единственного μ в первом смысле, и наоборот, всякое μ в первом смысле «ограничивается» до некоторого μ во втором смысле. Точнее, пусть μ — распределение

в смысле первого определения. Тогда, положив

$$\mu(U) = \int (\text{характеристическая функция подмножества } U)\,\mu$$

для каждого компактно-открытого подмножества U, мы получим распределение (также обозначаемое через μ) в смысле второго определения. Обратно, если мы имеем распределение μ в смысле второго определения, то соответствующее распределение в первом смысле задается $\mathbb{Q}_p$-линейным продолжением с множества характеристических функций, для которых полагаем

$$\int (\text{характеристическая функция подмножества } U)\,\mu = \mu(U).$$

Итак, значение $\int f\mu$ для локально постоянной f легко вычислить, зная разложение f в линейную комбинацию характеристических функций.

Предложение. *Каждое отображение μ множества интервалов, содержащихся в X, в $\mathbb{Q}_p$, для которого*

$$\mu(a+(p^N)) = \sum_{b=0}^{p-1} \mu(a+bp^N+(p^{N+1}))$$

при любом $a+(p^N) \subset X$, однозначно продолжается до p-адического распределения на X.

Доказательство. Каждое компактно-открытое подмножество $U \subset X$ можно представить в виде конечного объединения непересекающихся интервалов: $U = \bigcup I_i$ (см. упр. 1). Положим тогда $\mu(U) \underset{\text{def}}{=} \sum \mu(I_i)$. (В силу аддитивности искомого μ, это значение $\mu(U)$ единственно возможное.) Проверим теперь независимость $\mu(U)$ от выбора разбиения множества U на интервалы. Для этого заметим прежде всего, что любые два разбиения $U = \bigcup I_i$ и $U = \bigcup I'_i$ на непересекающиеся интервалы имеют общее подразбиение (более мелкое, чем каждое из исходных) $I_i = \bigcup_j I_{ij}$, причем если $I_i = a+(p^N)$, то

I_{ij} пробегает все интервалы вида $a'+(p^{N'})$, где N' — некоторое фиксированное натуральное число $>N$, а $a'\equiv a \pmod{p^N}$. Тогда, применяя несколько раз формулу из условий предложения, мы получаем

$$\mu(I_i)=\mu(a+(p^N))=\sum_{j=0}^{p^{N'-N}-1}\mu(a+jp^N+(p^{N'}))=$$

$$=\sum_j \mu(I_{ij}).$$

Следовательно, $\sum_i \mu(I_i)=\sum_{i,j}\mu(I_{ij})$. Отсюда $\sum_i \mu(I_i)=$ $=\sum_i \mu(I'_i)$, потому что обе части равны сумме по общему подразбиению. Теперь аддитивность μ очевидна. А именно, пусть U—объединение непересекающихся U_i. Разобьем каждое U_i в объединение непересекающихся интервалов I_{ij}. Тогда $U=\bigcup_{i,j} I_{ij}$ и

$$\mu(U)=\sum_{i,j}\mu(I_{ij})=\sum_i\sum_j\mu(I_{ij})=\sum_i\mu(U_i).\ \square$$

Приведем теперь несколько простых примеров p-адических распределений.

(1) Распределение Хаара μ_{Haar}. Положим

$$\mu_{\text{Haar}}(a+(p^N))\underset{\text{def}}{=}\frac{1}{p^N}.$$

По предыдущему предложению, эта функция продолжается до распределения на $\mathbb{Z}_p$, так как

$$\sum_{b=0}^{p-1}\mu_{\text{Haar}}(a+bp^N+(p^{N+1}))=\sum_{b=0}^{p-1}\frac{1}{p^{N+1}}=\frac{1}{p^N}=$$

$$=\mu_{\text{Haar}}(a+(p^N)).$$

Это единственное (с точностью до постоянного множителя) распределение, *инвариантное относительно сдвигов*, т. е. такое, что $\mu_{\text{Haar}}(a+U)=\mu_{\text{Haar}}(U)$ для всех $a\in\mathbb{Z}_p$, где $a+U\underset{\text{def}}{=}\{x\in\mathbb{Z}_p \mid x-a\in U\}$.

(2) Распределение Дирака μ_α, сосредоточенное в точке $\alpha \in \mathbb{Z}_p$ (α фиксировано). Положим

$$\mu_\alpha(U) \underset{\text{def}}{=} \begin{cases} 1, & \text{если } \alpha \in U, \\ 0 & \text{в противном случае.} \end{cases}$$

Аддитивность μ_α очевидна. Отметим, что $\int f\mu_\alpha = f(\alpha)$ для локально постоянных функций f.

(3) Распределение Мазура μ_{Mazur}. Прежде всего без ограничения общности запишем каждый интервал из $\mathbb{Z}_p$ в виде $a+(p^N)$, где a — целое рациональное число между 0 и p^N-1. Предполагая это, зададим

$$\mu_{\text{Mazur}}(a+(p^N)) \underset{\text{def}}{=} \frac{a}{p^N} - \frac{1}{2}.$$

Проверку аддитивности для μ_{Mazur} отложим до следующего параграфа, в котором она окажется частным случаем некоторого более общего утверждения.

В заключение укажем на одно существенное отличие распределений μ_{Haar} и μ_{Mazur} от классических мер. В этих двух примерах p-адических распределений мера «стягивающегося» интервала (т. е. при $N \to \infty$) *увеличивается* в p-адической метрике, а именно:

$$|\mu_{\text{Haar}}(a+(p^N))|_p = \left|\frac{1}{p^N}\right|_p = p^N$$

и для $p \nmid a$ (и $N > 1$ в случае $p = 2$)

$$|\mu_{\text{Mazur}}(a+(p^N))|_p = \left|\frac{a}{p^N} - \frac{1}{2}\right|_p = p^N.$$

С этой особенностью мы еще столкнемся ниже.

Упражнения

1. Дайте прямое доказательство компактности $\mathbb{Z}_p$ (т. е. существования конечного подпокрытия для каждого открытого покрытия $\mathbb{Z}_p$). Затем докажите, что открытое подмножество в $\mathbb{Z}_p$ компактно тогда и только тогда, когда оно представимо в виде конечного объединения непересекающихся интервалов. Заметим, что каждый интервал представим в виде конечного объединения

непересекающихся интервалов «равной длины»: $a+(p^n)=\bigcup_{b=0}^{p-1} a+bp^n+(p^{n+1})$. Докажите, что конечное повторное применение последней процедуры позволяет получить любое разбиение интервала в объединение непересекающихся подынтервалов.

2. Приведите пример открытого некомпактного подмножества в $\mathbb{Z}_p$.

3. Пусть U — открытое подмножество топологического пространства X, а $f\colon X\to\mathbb{Z}$ — его характеристическая функция, т. е.

$$f(x)=\begin{cases}1, & \text{если } x\in X,\\ 0 & \text{в противном случае.}\end{cases}$$

Покажите, что f локально постоянна для $X=\mathbb{Z}_p$ и любого компактно-открытого подмножества U, но не локально постоянна, если $X=\mathbb{R}$ и U — непустое открытое подмножество, отличное от $\mathbb{R}$.

4. Пусть X — компактно-открытое подмножество в $\mathbb{Q}_p$. Покажите, что функция $f\colon X\to\mathbb{Q}_p$ локально постоянна тогда и только тогда, когда она равна конечной линейной комбинации с коэффициентами в $\mathbb{Q}_p$ характеристических функций компактно-открытых подмножеств в X. Затем докажите эквивалентность двух определений распределения на X.

5. Пусть $\alpha\in\mathbb{Q}_p$ и $|\alpha|_p=1$. Покажите, что $\mu_{\text{Haar}}(\alpha U)=\mu_{\text{Haar}}(U)$ для каждого открытого компактного подмножества U, где αU обозначает множество $\{\alpha x \mid x\in U\}$.

6. Пусть $f\colon \mathbb{Z}_p\to\mathbb{Q}_p$ — локально постоянная функция, заданная следующим способом: $f(x)=$ первый знак p-адического разложения x. Найдите $\int f\mu$, когда: (1) $\mu=$ распределение Дирака μ_a; (2) $\mu=\mu_{\text{Haar}}$; (3) $\mu=\mu_{\text{Mazur}}$.

7. Пусть μ — функция на множестве интервалов $a+(p^N)$, заданная формулой

$$\mu(a+(p^N))=\begin{cases}p^{-[(N+1)/2]}, & \text{если первые } [N/2] \text{ знаков при нечетных степенях } p \text{ в } p\text{-адическом разложении } a \text{ равны 0,}\\ 0 & \text{в противном случае,}\end{cases}$$

где $[\ ]$ — целая часть. Докажите, что μ продолжается до распределения на $\mathbb{Z}_p$.

8. Обдумайте, как можно было бы построить примеры p-адических распределений с разной степенью роста $\max_{0\leqslant a<p^N}|\mu(a+(p^N))|_p$ при возрастании N.

§ 4. РАСПРЕДЕЛЕНИЯ БЕРНУЛЛИ

Прежде всего определим многочлены Бернулли $B_k(x)$. Рассмотрим следующую функцию от двух переменных t и x:

$$\frac{te^{xt}}{e^t-1}=\left(\sum_{k=0}^{\infty}B_k\frac{t^k}{k!}\right)\left(\sum_{k=0}^{\infty}\frac{(xt)^k}{k!}\right).$$

Собирая коэффициенты этого произведения при t^k, мы получим для каждого k многочлен от x. Произведение этого многочлена на $k!$ называется k-м многочленом Бернулли и обозначается через $B_k(x)$. Таким образом,

$$\frac{te^{xt}}{e^t-1}=\sum_{k=0}^{\infty}B_k(x)\frac{t^k}{k!}.$$

Вот несколько первых многочленов Бернулли:

$$B_0(x)=1,\quad B_1(x)=x-{}^1/_2,\quad B_2(x)=x^2-x+{}^1/_6,$$
$$B_3=x^3-{}^1/_2x^2+{}^3/_2x,\ \ldots\ .$$

В этом параграфе, употребляя обозначение $a+(p^N)$, мы подразумеваем, что $0\leqslant a\leqslant p^N-1$. Фиксируем некоторое целое неотрицательное число k и определим отображение $\mu_{B,k}$ на множестве интервалов $a+(p^N)$ формулой

$$\mu_{B,k}(a+(p^N))=p^{N(k-1)}B_k(a/p^N).$$

Предложение. *Функция $\mu_{B,k}$ продолжается до распределения на $\mathbb{Z}_p$ (называемого k-м распределением Бернулли).*

Доказательство. По предложению из § 3 достаточно показать, что

$$\mu_{B,k}(a+(p^N))=\sum_{b=0}^{p-1}\mu_{B,k}(a+bp^N+(p^{N+1})).$$

Правая часть равна

$$p^{(N+1)(k-1)}\sum_{b=0}^{p-1}B_k\left(\frac{a+bp^N}{p^{N+1}}\right).$$

Умножим доказываемое соотношение на $p^{-N(k-1)}$ и положим $\alpha = a/p^{N+1}$. Тогда мы увидим, что необходимо доказать соотношение

$$B_k(p\alpha) = p^{k-1} \sum_{b=0}^{p-1} B_k\left(\alpha + \frac{b}{p}\right).$$

Правая часть, деленная на $k!$, равна по определению многочленов $B_k(x)$ коэффициенту при t^k в разложении Тейлора функции

$$p^{k-1} \sum_{b=0}^{p-1} \frac{te^{(\alpha+b/p)t}}{e^t-1} = \frac{p^{k-1}te^{\alpha t}}{e^t-1} \sum_{b=0}^{p-1} e^{bt/p} = \frac{p^{k-1}te^{\alpha t}}{e^t-1} \cdot \frac{e^t-1}{e^{t/p}-1}.$$

Последний сомножитель получается суммированием геометрической прогрессии $\sum_{b=0}^{p-1} e^{bt/p}$. Далее находим

$$\frac{p^k (t/p) e^{(p\alpha)t/p}}{e^{t/p}-1} = p^k \sum_{j=0}^{\infty} B_j(p\alpha) \frac{(t/p)^j}{j!}$$

снова по определению $B_j(x)$. Следовательно, $k!$ раз взятый коэффициент этого ряда при t^k совпадает с

$$p^k B_k(p\alpha)\left(\frac{1}{p}\right)^k = B_k(p\alpha),$$

что и требовалось доказать. □

Несколько первых многочленов $B_k(x)$ дают следующие распределения:

$\mu_{B,0}(a+(p^N)) = p^{-N}$, т. е. $\mu_{B,0} = \mu_{\text{Haar}}$;

$\mu_{B,1}(a+(p^N)) = B_1\left(\frac{a}{p^N}\right) = \frac{a}{p^N} - \frac{1}{2}$, т. е. $\mu_{B,1} = \mu_{\text{Mazur}}$;

$\mu_{B,2}(a+(p^N)) = p^N\left(\frac{a^2}{p^{2N}} - \frac{a}{p^N} + \frac{1}{6}\right)$ и т. д.

Можно показать, что среди всех многочленов многочлены Бернулли единственные (с точностью до постоянного множителя), для которых можно задать распределения указанным выше способом. Этот факт нам не понадобится, поэтому мы его не доказываем. Однако

следует отметить важную и уникальную роль многочленов Бернулли $B_k(x)$ в p-адическом интегрировании. Это окажется связанным с появлением чисел Бернулли B_k (которые являются постоянными членами $B_k(x)$; см. ниже упр. 1) в доказанной выше формуле для $\zeta(2k)$.

§ 5. МЕРЫ И ИНТЕГРИРОВАНИЕ

Определение. *Мерой* называется p-адическое распределение μ на X, значения которого на открытых компактных подмножествах $U \subset X$ ограничены некоторой константой $B \in \mathbb{R}$, т. е.

$$|\mu(U)|_p \leqslant B \quad \text{для всех компактно-открытых } U \subset X.$$

Распределение Дирака μ_a для любого фиксированного $a \in \mathbb{Z}_p$ является мерой, но ни одно из распределений Бернулли не обладает этим свойством. Для превращения распределений Бернулли в меры существует стандартная процедура, называемая *регуляризацией*. Прежде всего введем некоторые обозначения. Для каждого $\alpha \in \mathbb{Z}_p$ обозначим через $\{\alpha\}_N$ целое рациональное число между 0 и $p^N - 1$, сравнимое с $\alpha \pmod{p^N}$. Для $\alpha \in \mathbb{Q}_p$ и распределения μ обозначим через $\alpha\mu$ произведение этого распределения на α, т. е. $(\alpha\mu)(U) = \alpha \cdot (\mu(U))$ для каждого компактно-открытого подмножества U. И, наконец, если $U \subset \mathbb{Q}_p$ — компактно-открытое подмножество, $\alpha \in \mathbb{Q}_p$ и $\alpha \neq 0$, то положим $\alpha U \overset{\text{def}}{=} \{x \in \mathbb{Q}_p \mid x/\alpha \in U\}$. Легко проверить, что сумма двух распределений (или мер) является распределением (соответственно мерой), произведение $\alpha\mu$ распределения (или меры) μ на скаляр является распределением (соответственно мерой), а кроме того, если $\alpha \in \mathbb{Z}_p^\times$, а μ — распределение (или мера) на $\mathbb{Z}_p$, то функция μ': $\mu'(U) = \mu(\alpha U)$ задает распределение (соответственно меру) на $\mathbb{Z}_p$.

Рассмотрим целое рациональное a, отличное от 1 и не делящееся на p. *Регуляризованное* распределение Бернулли $\mu_{B,k,a}$ на $\mathbb{Z}$, или, короче, $\mu_{k,a}$, определяется формулой

$$\mu_{k,a}(U) \overset{\text{def}}{=} \mu_{B,k}(U) - a^{-k}\mu_{B,k}(aU).$$

Вскоре мы установим, что $\mu_{k,a}$ — мера. Во всяком случае, как следует из замечаний в конце предыдущего абзаца, это заведомо распределение.

Его легко вычислить явно при $k=0$ или 1. Если $k=0$, то $\mu_{B,0}=\mu_{\text{Haar}}$ и, очевидно, $\mu_{0,a}(U)=0$ для любого U (см. упр. 5 к § 3). При $k=1$ получаем

$$\mu_{1,a}(a+(p^N)) = \frac{a}{p^N} - \frac{1}{2} - \frac{1}{\alpha}\left(\frac{\{\alpha a\}_N}{p^N} - \frac{1}{2}\right) =$$

$$= \frac{(1/\alpha-1)}{2} + \frac{a}{p^N} - \frac{1}{\alpha}\left(\frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N}\right]\right) = \frac{1}{\alpha}\left[\frac{\alpha a}{p^N}\right] + \frac{(1/\alpha)-1}{2}$$

(где [ ] обозначает целую часть).

Предложение. *Для всех компактно-открытых* $U \subset \mathbb{Z}_p$

$$|\mu_{1,a}(U)|_p \leqslant 1.$$

Доказательство. Отметим, что $(\alpha^{-1}-1)/2 \in \mathbb{Z}_p$, так как $1/\alpha \in \mathbb{Z}_p$ и $1/2 \in \mathbb{Z}_p$, если $p \neq 2$. В случае $p=2$ верно то же самое, потому что $\alpha^{-1}-1 \equiv 0 \pmod 2$. Так как $[\alpha a/p^N] \in \mathbb{Z}$, то по предыдущей формуле $\mu_{1,a}(a+(p^N)) \in \mathbb{Z}_p$. С другой стороны, любое компактно-открытое множество U представимо в виде конечного объединения непересекающихся интервалов I_i. Поэтому $|\mu_{1,a}(U)|_p \leqslant \max |\mu_{1,a}(I_i)|_p \leqslant 1$. □

Итак, $\mu_{1,a}$ — мера. Это первый встретившийся нам интересный пример p-адической меры. Вскоре мы увидим, что мера $\mu_{1,a}$ играет почти такую же фундаментальную роль в p-адическом интегрировании, как «dx» в случае вещественного интегрирования.

Ниже мы докажем основное сравнение, связывающее распределения $\mu_{k,a}$ и $\mu_{1,a}$. Его доказательство на первый взгляд кажется просто непривлекательным вычислением, но оно становится понятнее, если рассмотреть аналогичную ситуацию из вещественного анализа. Предположим, что мы вычисляем интеграл вида $\int f\left(\sqrt[k]{x}\right) dx$ и хотим сделать замену переменных $x \longmapsto x^k$, т. е. перейти к вычислению интеграла $\int f(x)\, d(x^k)$. Далее используется простое правило: $d(x^k)/dx = kx^{k-1}$. На самом деле $d(x^k)$ можно рассматривать как «меру» μ_k

на вещественной прямой, для которой $\mu_k([a, b]) = b^k - a^k$. Тогда μ_1 является обычной длиной. Соотношение $d(x^k)/dx = kx^{k-1}$ в сущности означает, что

$$\lim_{b \to a} \mu_k([a, b])/\mu_1([a, b]) = ka^{k-1}.$$

Следовательно, заменяя $\mu_k(I_i)$ на $kx_i^{k-1}\mu_1(I_i)$ в интегральных суммах Римана $\sum f(x_i)\mu_k(I_i)$, мы получим при уменьшении длин всех I_i в пределе $\int f(x)\,kx^{k-1}dx$.

В доказательстве этого предельного соотношения используется биномиальное разложение для $(a+h)^k$ (где $h = b - a$). В действительности важны только первые два члена этого разложения: $a^k + kha^{k-1}$. Подобно этому в p-адическом случае при доказательстве асимптотической формулы $\mu_{k,a}(I) \sim ka^{k-1}\mu_{1,a}(I)$ для малых интервалов I, содержащих a, также используется биномиальное разложение. Таким образом, теорему 5 следует рассматривать как аналог теоремы из анализа, утверждающей, что $d(x^k)/dx = kx^{k-1}$. (При этом можно не обращать внимания на множители d_k в обеих частях сравнения из теоремы 5. Они означают лишь, что если разделить обе части на d_k, то p^N заменится на $p^{N - \operatorname{ord}_p d_k}$, где $\operatorname{ord}_p d_k$ — *константа*, не существенная при больших N.)

Теорема 5. *Пусть d_k — наименьшее общее кратное знаменателей всех коэффициентов многочлена $B_k(x)$: $d_1 = 2$, $d_2 = 6$, $d_3 = 2$ и т. д. Тогда*

$$d_k\mu_{k,a}(a + (p^N)) \equiv d_k\, ka^{k-1}\mu_{1,a}(a + (p^N)) \pmod{p^N}.$$

Доказательство. Из упр. 1 ниже следует, что многочлен $B_k(x)$ начинается с

$$B_0x^k + kB_1x^{k-1} + \ldots = x^k - \frac{k}{2}x^{k-1} + \ldots.$$

По определению,

$$d_k\mu_{k,a}(a + (p^N)) = d_kp^{N(k-1)}\left(B_k\left(\frac{a}{p^N}\right) - a^{-k}B_k\left(\frac{\{\alpha a\}_N}{p^N}\right)\right).$$

Многочлен $d_kB_k(x)$ имеет целые коэффициенты и степень k. Поэтому в дальнейших рассмотрениях можно

учитывать только два его старших члена $d_k x^k - d_k (k/2) x^{k-1}$, ибо, так как x имеет знаменатель p^N, все остальные члены после умножения на $p^{N(k-1)}$ становятся целыми, делящимися на p^N. Кроме того, отметим, что $\alpha a \equiv \{\alpha a\}_N \pmod{p^N}$ и

$$\frac{\{\alpha a\}_N}{p^N} = \frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N}\right] \quad ([\ ] - \text{целая часть}).$$

Следовательно,

$$d_k \mu_{k,\alpha}(a+(p^N)) \equiv d_k p^{N(k-1)} \left(\frac{a^k}{p^{Nk}} - \alpha^{-k}\left(\frac{\{\alpha a\}_N}{p^N}\right)^k - \right.$$

$$\left. - \frac{k}{2}\left(\frac{a^{k-1}}{p^{N(k-1)}} - \alpha^{-k}\left(\frac{\{\alpha a\}_N}{p^N}\right)^{k-1}\right)\right) \pmod{p^N} =$$

$$= d_k \left(\frac{a^k}{p^N} - \alpha^{-k} p^{N(k-1)} \left(\frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N}\right]\right)^k - \right.$$

$$\left. - \frac{k}{2}\left(a^{k-1} - \alpha^{-k} p^{N(k-1)} \left(\frac{\alpha a}{p^N} - \left[\frac{\alpha a}{p^N}\right]\right)^{k-1}\right)\right) \equiv$$

$$\equiv d_k \left(\frac{a^k}{p^N} - \alpha^{-k}\left(\frac{\alpha^k a^k}{p^N} - k\alpha^{k-1} a^{k-1}\left[\frac{\alpha a}{p^N}\right]\right) - \right.$$

$$\left. - \frac{k}{2}\left(a^{k-1} - \alpha^{-k}\left(\alpha^{k-1} a^{k-1}\right)\right)\right) \pmod{p^N} =$$

$$= d_k k a^{k-1} \left(\frac{1}{\alpha}\left[\frac{\alpha a}{p^N}\right] + \frac{1/\alpha - 1}{2}\right) =$$

$$= d_k k a^{k-1} \mu_{1,\alpha}(a+(p^N)). \quad \square$$

Следствие. *Распределение* $\mu_{k,\alpha}$ *является мерой для любого* $k = 1, 2, 3, \ldots$ *и любого* $\alpha \in \mathbb{Z}$, $\alpha \notin p\mathbb{Z}$, $\alpha \neq 1$.

Доказательство. Мы должны установить ограниченность чисел $\mu_{k,\alpha}(a+(p^N))$. По теореме 5

$$|\mu_{k,\alpha}(a+(p^N))|_p \leqslant \max\left(\left|\frac{p^N}{d_k}\right|_p,\ |k a^{k-1} \mu_{1,\alpha}(a+(p^N))|_p\right) \leqslant$$

$$\leqslant \max\left(\left|\frac{1}{d_k}\right|_p,\ |\mu_{1,\alpha}(a+(p^N))|_p\right).$$

Но $|\mu_{1,\alpha}(a+(p^N))|_p \leqslant 1$, а d_k фиксировано. $\square$

Для чего же мы суетились и превратили (регуляризовали) распределения Бернулли в меры? Дело в том, что если μ — неограниченное распределение, то интеграл $\int f\mu$ определен лишь для локально постоянных функций f, и при попытках распространить интегрирование на непрерывные функции, рассматривая пределы римановых сумм, возникают трудности.

Возьмем, например, $\mu = \mu_{\text{Haar}}$ и простейшую функцию $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$, $f(x) = x$. Построим римановы суммы. Для заданной функции f и каждого N разобьем $\mathbb{Z}_p$ в объединение $\bigcup_{a=0}^{p^N-1} (a + (p^N))$, выберем в a-м интервале произвольную точку $x_{a,N}$ и определим N-ю риманову сумму функции f, соответствующую выбору точек $\{x_{a,N}\}$, как

$$S_{N,\{x_{a,N}\}}(f) \underset{\text{def}}{=} \sum_{a=0}^{p^N-1} f(x_{a,N})\mu(a + (p^N)).$$

В нашем примере эта сумма равна $\sum_{a=0}^{p^N-1} x_{a,N}\frac{1}{p^N}$. Например, при простейшем выборе $x_{a,N} = a$ получим

$$p^{-N}\sum_{a=0}^{p^N-1} a = p^{-N}\frac{(p^N-1)(p^N)}{2} = \frac{p^N-1}{2}.$$

При $N \to \infty$ эта сумма имеет предел в $\mathbb{Q}_p$, равный $-1/2$. Но если одно из выбранных значений $x_{a,N} = a \in a + (p^N)$ заменить на $a + a_0p^N \in a + (p^N)$ для каждого N, где a_0 — некоторое фиксированное целое p-адическое число, то мы получим

$$p^{-N}\left(\sum_{a=0}^{p^N-1} a + a_0p^N\right) = \frac{p^N-1}{2} + a_0,$$

что стремится к $a_0 - 1/2$. Следовательно, в этом случае римановы суммы не имеют предела, который бы не зависел от выбора точек в интервалах.

От «меры» μ мало толку, и она даже не заслуживает названия меры, если по ней нельзя проинтегрировать непрерывную функцию. (Здесь мы слегка преувеличиваем, см. ниже упр. 8 — 10.) Покажем теперь, что с этой точки зрения ограниченные распределения имеют право называться «мерами».

Напомним, что через X обозначается компактно-открытое подмножество в $\mathbb{Q}_p$, такое, например, как $\mathbb{Z}_p$ или $\mathbb{Z}_p^\times$. (Для простоты предположим, что $X \subset \mathbb{Z}_p$.)

Теорема 6. *Пусть μ — некоторая p-адическая мера на X, а $f\colon X \to \mathbb{Q}_p$ — непрерывная функция. Тогда существует предел при $N \to \infty$ римановых сумм*

$$S_{N,\{x_{a,N}\}} \underset{\text{def}}{=} \sum_{\substack{0 \leqslant n < p^N \\ n + (p^N) \subset X}} f(x_{a,N})\,\mu(a + (p^N))$$

(где суммирование ведется по всем a, для которых $a + (p^N) \subset X$, а $x_{a,N}$ — точки, выбранные в $a + (p^N)$), и этот предел не зависит от выбора $\{x_{a,N}\}$.

Доказательство. Предположим, что $|\mu(U)|_p \leqslant B$ для всех компактно-открытых подмножеств $U \subset X$. Оценим вначале $|S_{N,\{x_{a,N}\}} - S_{M,\{x_{a,M}\}}|_p$ при $M > N$. Выберем настолько большое натуральное N, что каждый интервал $a + (p^N)$ либо содержится в X, либо не пересекается с ним. Это возможно в силу представимости X в виде конечного объединения интервалов. Пользуясь аддитивностью μ, запишем $S_{N,\{x_{a,N}\}}$ следующим образом:

$$\sum_{\substack{0 \leqslant a < p^M \\ a + (p^M) \subset X}} f(x_{\bar{a},N})\,\mu(a + (p^M))$$

(где $\bar{a}$ обозначает приведенный вычет числа a по модулю p^N [1])). Кроме того, будем считать N настолько большим, что $|f(x) - f(y)|_p < \varepsilon$, когда $x \equiv y \pmod{p^N}$. (Отметим, что, поскольку X *компактно*, из непрерывности следует *равномерная* непрерывность; доказательство легко провести самостоятельно или можно обратиться к книге

[1]) То есть наименьшее целое неотрицательное число, сравнимое с a по модулю p^N. — *Прим. перев.*

Симмонса [(a) 1][1].) Тогда

$$|S_{N,\{x_{a,N}\}} - S_{M,\{x_{a,M}\}}|_p = \left| \sum_{\substack{0 \leqslant a < p^M \\ a+(p^M) \subset X}} (f(x_{\bar{a},N}) - f(x_{a,M}))\,\mu(a+(p^M)) \right|_p \leqslant$$
$$\leqslant \max\left(|f(x_{\bar{a},N}) - f(x_{a,M})|_p \cdot |\mu(a+(p^M))|_p\right) \leqslant \varepsilon B,$$

так как $x_{\bar{a},N} \equiv x_{a,M} \pmod{p^N}$. Поскольку B фиксировано, а ε произвольно, предел римановых сумм существует.

Независимость от выбора $\{x_{a,N}\}$ доказывается аналогично. А именно

$$|S_{N,\{x_{a,N}\}} - S_{N,\{x'_{a,N}\}}|_p = \left| \sum_{\substack{0 \leqslant a < p^N \\ a+(p^N) \subset X}} (f(x_{a,N}) - f(x'_{a,N}))\,\mu(a+(p^N)) \right|_p \leqslant$$
$$\leqslant \max_a\left(|f(x_{a,N}) - f(x'_{a,N})|_p \cdot |\mu(a+(p^N))|_p\right) \leqslant \varepsilon B. \quad \square$$

Определение. Пусть $f\colon X \to \mathbb{Q}_p$ — непрерывная функция, а μ — некоторая мера на X. Определим $\int f\mu$ как предел римановых сумм, существование которого было только что установлено. (Отметим, что так определенный интеграл совпадает с введенным ранее $\int f\mu$ для локально постоянных функций f.)

Следующие простые, но важные утверждения получаются непосредственно из этого определения.

Предложение. *Если $f\colon X \to \mathbb{Q}_p$ — такая непрерывная функция, что $|f(x)|_p \leqslant A$ для всех $x \in X$, а $|\mu(U)|_p \leqslant B$ для всех компактно-открытых подмножеств $U \subset X$, то*

$$\left|\int f\mu\right|_p \leqslant A \cdot B.$$

Следствие. *Если $f, g\colon X \to \mathbb{Q}_p$ — две такие непрерывные функции, что $|f(x) - g(x)|_p \leqslant \varepsilon$ для всех $x \in X$, а $|\mu(U)|_p \leqslant B$ для всех компактно-открытых подмножеств $U \subset X$, то*

$$\left|\int f\mu - \int g\mu\right|_p \leqslant \varepsilon B.$$

[1]) См. также [(a) 5]. — *Прим. перев.*

Упражнения

1. Покажите, что $B_k(x) = \sum_{i=0}^{k} \binom{k}{i} B_i x^{k-i}$ и, в частности, $B_k(0) = B_k$. Кроме того, покажите, что

$$\int_0^1 B_k(x)\,dx = \begin{cases} 1, & \text{если } k=0, \\ 0, & \text{если } k \neq 0, \end{cases} \quad \text{и} \quad \frac{d}{dx} B_k(x) = kB_{k-1}(x).$$

2. Докажите, что не существует распределения μ (кроме тождественно равного нулю), которое обладало бы следующим свойством:

$$\max_{0 \leqslant a < p^N} |\mu(a + (p^N))|_p \to 0 \quad \text{при} \quad N \to \infty.$$

3. Чему равно $\mu_{B,k}(\mathbb{Z}_p)$? $\mu_{B,k}(p\mathbb{Z}_p)$? $\mu_{B,k}(\mathbb{Z}_p^\times)$?

4. Докажите, что p-адическое распределение μ является мерой тогда и только тогда, когда при некотором $a \in \mathbb{Z}_p$ распределение $a \cdot \mu$ принимает значения в $\mathbb{Z}_p$. Докажите, что меры на X образуют векторное пространство над $\mathbb{Q}_p$.

5. Выразите $\mu_{k,\alpha}(\mathbb{Z}_p)$ и $\mu_{k,\alpha}(\mathbb{Z}_p^\times)$ через α и k. Вычислите $\int_{\mathbb{Z}_p^\times} f\mu_{1,\alpha}$ для $f(x) = \sum_{i=0}^{n} a_i x^i$.

6. Пусть p — нечетное простое число. Для $a = 0, 1, \ldots, p^n - 1$ обозначим через S_a сумму p-адических знаков числа a. Докажите, что функция $\mu(a + (p^n)) = (-1)^{S_a}$ определяет меру на $\mathbb{Z}_p$ и что $\int f\mu = 0$ для любой нечетной функции f (т. е. такой, что $f(-x) = -f(x)$).

7. Пусть $p > 2$, $f(x) = 1/x$ и $\alpha = 1 + p$. Докажите, что $\int_{\mathbb{Z}_p^\times} f\mu_{1,\alpha} \equiv -1 \pmod{p}$. (*Указание.* Воспользуйтесь следствием в конце § 5 с $g(x) = 1/(\text{первый знак } x)$, так что $\langle x \rangle \equiv g(x) \pmod{p}$, а $g(x)$ локально постоянна.)

8. Распределение μ на X называется *распределением ограниченного роста*, если $\max_{0 \leqslant a < p^N} |p^N \mu(a + (p^N))|_p \to 0$ при $N \to \infty$, т. е. μ «возрастает строго медленнее, чем μ_{Haar}». Докажите справедливость теоремы 6 для таких μ и функций $f\colon X \to \mathbb{Q}_p$, удовлетворяющих условию Липшица: существует $A \in \mathbb{R}$ со свойством

$$|f(x) - f(y)|_p \leqslant A\,|x - y|_p \quad \text{при любых} \quad x, y \in X.$$

(Это понятие ввел Ю. И. Манин и применил его к p-адической интерполяции рядов Гекке.)

9. Пусть μ — распределение из упр. 7 к § 3. Проверьте, что μ имеет ограниченный рост. Пусть $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ — функция $f(x) = x$. Вычислите интеграл $\int f\mu$, который определен в силу предыдущего упражнения.

10. Пусть r — некоторое вещественное положительное число. Функцию $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ Мазур называет функцией «типа r», если существует такое $A \in \mathbb{R}$, что

$$|f(x) - f(x')|_p \leqslant A\,|x - x'|_p^r \quad \text{для всех} \quad x, x' \in \mathbb{Z}_p.$$

Отметим, что каждая такая фуикция непрерывна. Если $r \geqslant 1$, то f удовлетворяет условию Липшица (см. упр. 8). Рассмотрим p-адическое распределение μ на $\mathbb{Z}_p$, такое, что

$$p^{-Ns} \max_{0 \leqslant a < p^N} |\mu(a + (p^N))|_p \to 0 \quad \text{при} \quad N \to \infty$$

для некоторого положительного $s \in \mathbb{R}$. Докажите аналог теоремы 6 для такого μ и функций типа r, когда $r \geqslant s$.

§ 6. p-АДИЧЕСКАЯ ζ-ФУНКЦИЯ КАК ПРЕОБРАЗОВАНИЕ МЕЛЛИНА — МАЗУРА

Пусть X — компактно-открытое подмножество в $\mathbb{Z}_p$. Каждую заданную на $\mathbb{Z}_p$ меру μ можно ограничить на X. Это ограничение μ^* на X определяется как мера с $\mu^*(U) = \mu(U)$ для любого компактно-открытого подмножества $U \subset X$. В применении к интегрированию это означает, что

$$\int f\mu^* = \int f \cdot (\text{характеристическая функция } X)\,\mu.$$

Интеграл $\int f\mu^*$ будет обозначаться через $\int\limits_X f\mu$.

Как уже было сказано, мы хотим проинтерполировать значения $-B_k/k$. Имеет место следующее простое соотношение:

$$\int 1 \cdot \mu_{B,\,k} = \mu_{B,\,k}(\mathbb{Z}_p) = B_k$$

(см. упр. 3 к § 5). Следовательно, нужно проинтерполировать числа $-\frac{1}{k}\int 1 \cdot \mu_{B,\,k}$.

Имеется ли непосредственная связь между распределениями $\mu_{B,\,k}$ при различных k? По-видимому, нет,

однако *регуляризованные* меры $\mu_{k,a}$ и $\mu_{1,a}$ связаны между собой по теореме 5. Точнее, из теорем 5 и 6 вытекает следующее

Предложение. *Пусть* $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ *— функция* $f(x) = x^{k-1}$ *(для фиксированного целого положительного* k*), а* X *— компактно-открытое подмножество в* $\mathbb{Z}_p$*. Тогда*

$$\int_X 1 \cdot \mu_{k,a} = k \int_X f\mu_{1,a}.$$

Доказательство. По теореме 5

$$\mu_{k,a}(a+(p^N)) \equiv ka^{k-1}\mu_{1,a}(a+(p^N)) \pmod{p^{N-\operatorname{ord}_p d_k}}.$$

Рассмотрим теперь настолько большое N, что X равно объединению интервалов вида $a+(p^N)$. Тогда

$$\int_X 1 \cdot \mu_{k,a} = \sum_{\substack{0 \leqslant a < p^N \\ a+(p^N) \subset X}} \mu_{k,a}(a+(p^N)) \equiv$$

$$\equiv \sum_{\substack{0 \leqslant a < p^N \\ a+(p^N) \subset X}} ka^{k-1}\mu_{1,a}(a+(p^N)) \pmod{p^{N-\operatorname{ord}_p d_k}} =$$

$$= k \sum_{\substack{0 \leqslant a < p^N \\ a+(p^N) \subset X}} f(a)\,\mu_{1,a}(a+(p^N)).$$

Переходя к пределу при $N \to \infty$, мы получаем требуемое соотношение $\int_X 1 \cdot \mu_{k,a} = k \int_X f\mu_{1,a}$. □

Если мы заменим в наших обозначениях f на x^{k-1}, считая x «переменной интегрирования», то результат предложения примет вид

$$\int_X 1 \cdot \mu_{k,a} = k \int_X x^{k-1}\mu_{1,a}.$$

Выражение справа гораздо приятнее левого с точки зрения p-адической интерполяции, потому что вместо загадочного индекса переменная интерполирования k превратилась в показатель степени.

В § 2 мы уже выяснили, когда и как можно проинтерполировать функцию x^{k-1} при фиксированном x

(см. также упр. 8 к § 2). А именно, для интерполяции пригодны только $x \not\equiv 0 \pmod p$. Чтобы область интегрирования состояла только из таких чисел x, нужно взять $X = \mathbb{Z}_p^\times$.

Итак, утверждается, что значения $\int\limits_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,a}$ *можно* проинтерполировать. Чтобы добиться этого, скомбинируем результаты § 2 и следствия в конце § 5. Согласно следствию, если $|f(x) - x^{k-1}|_p \leqslant \varepsilon$ для всех $x \in \mathbb{Z}_p^\times$, то

$$\left| \int\limits_{\mathbb{Z}_p^\times} f\mu_{1,a} - \int\limits_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,a} \right|_p \leqslant \varepsilon$$

(напомним, что $|\mu_{1,a}(U)|_p \leqslant 1$ для каждого компактно-открытого подмножества U). Подставим вместо f функцию $x^{k'-1}$, для которой $k' \equiv k \pmod{p-1}$ и $k' \equiv k \pmod{p^N}$ (это равносильно выполнению одного сравнения $k' \equiv k \pmod{(p-1)p^N}$). Из рассуждений § 2 следует неравенство

$$|x^{k'-1} - x^{k-1}|_p \leqslant 1/p^{N+1}$$

для всех $x \in \mathbb{Z}_p^\times$. Поэтому

$$\left| \int\limits_{\mathbb{Z}_p^\times} x^{k'-1}\mu_{1,a} - \int\limits_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,a} \right|_p \leqslant \frac{1}{p^{N+1}}.$$

Итак, фиксируем $s_0 \in \{0, 1, 2, \ldots, p-2\}$. Пусть $S_{s_0} \overline{\text{def}}$ {целые положительные числа, сравнимые с s_0 по модулю $p-1$} — область изменения переменной k. Тогда из предыдущего мы заключаем, что функция $\int\limits_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,a}$ от k продолжается до непрерывной функции $\int\limits_{\mathbb{Z}_p^\times} x^{s_0+s(p-1)-1}\mu_{1,a}$ от целого p-адического s.

Однако мы ушли немного в сторону от исходных чисел $\frac{1}{k}\int 1 \cdot \mu_{B,k}$. Выше было установлено, что значения

$$\int\limits_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,a} = \frac{1}{k}\int\limits_{\mathbb{Z}_p^\times} 1 \cdot \mu_{k,a}$$

можно проинтерполировать. Сравним эти числа с исходными:

$$\frac{1}{k}\int\limits_{\mathbb{Z}_p^\times} 1\cdot\mu_{k,\,a} = \frac{1}{k}\,\mu_{k,\,a}(\mathbb{Z}_p^\times) = \frac{1}{k}\,(1-\alpha^{-k})\,(1-p^{k-1})\,B_k =$$

(см. упр. 5 к § 5)

$$= (\alpha^{-k}-1)\,(1-p^{k-1})\left(-\frac{1}{k}\int\limits_{\mathbb{Z}_p} 1\cdot\mu_{B,\,k}\right).$$

Множитель $1-p^{k-1}$ появился в силу того, что интегрировать пришлось по $\mathbb{Z}_p^\times$, а не по $\mathbb{Z}_p$. Этот эффект уже был предсказан в конце § 2: перед интерполяцией ζ-функции следует убрать эйлеров p-множитель, так как функция n^s при $p\,|\,n$ не интерполируется. Поэтому ниже мы будем интерполировать числа $(1-p^{k-1})\times$ $\times\,(-B_k/k)$:

$$(1-p^{k-1})\left(-\frac{B_k}{k}\right) = \frac{1}{\alpha^{-k}-1}\int\limits_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\,a}.$$

Как мы предупреждали в § 2, читателя не должен смущать вид эйлерова множителя $1-p^{k-1}$, хотя по эвристическим соображениям из § 2 следовало как будто ожидать множитель $1-p^{-k}$. Дело обстоит так, как если бы на самом деле интерполировались не значения $\zeta(k)$, а значения «$\zeta(1-k)$» (правда, мы их пока не определили при положительных k). Поэтому мы определим ниже p-адическую ζ-функцию так, чтобы она принимала значение $(1-p^{k-1})\,(-B_k/k)$ для целого числа $1-k$, а не для самого k.

Определение. Для целого положительного k пусть

$$\zeta_p(1-k) \overset{\text{def}}{=} (1-p^{k-1})\,(-B_k/k),$$

так что, по предыдущему,

$$\zeta_p(1-k) = \frac{1}{\alpha^{-k}-1}\int\limits_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\,a}.$$

Заметим, что правая часть последнего выражения не зависит от α. Действительно, если $\beta\in\mathbb{Z}$, $p\nmid\beta$,

$\beta \neq 1$, то $(\beta^{-k}-1)^{-1}\int\limits_{Z_p^\times} x^{k-1}\mu_{1,\beta} = (\alpha^{-k}-1)^{-1}\int\limits_{Z_p^\times} x^{k-1}\mu_{1,\alpha}$, так как оба эти числа равны $(1-p^{k-1})(-B_k/k)$. Это равенство, т. е. независимость от α, также можно доказать непосредственно (см. упр. 1). Независимость от α будет использована ниже при определении $\zeta_p(s)$ для p-адических s.

Прежде всего выведем несколько классических теоретикочисловых результатов о числах Бернулли. Эти результаты всегда считались очень изящными, но загадочными, пока не была открыта их связь с дзета-функцией Куботы — Леопольдта ζ_p и мерой Мазура $\mu_{1,\alpha}$, которая показала, что они возникают естественным образом из «аналитических» соображений (а именно, из следствия в конце § 5, которое, грубо говоря, утверждает, что две функции, близкие на некотором интервале, имеют близкие интегралы).

Теорема 7 ((1) и (2) — Куммер, (3) — Клаузен и фон Штаудт).

(1) *Если* $(p-1)\nmid k$, *то* $|B_k/k|_p \leqslant 1$.

(2) *Если* $(p-1)\nmid k$ *и* $k \equiv k' \pmod{(p-1)p^N}$, *то*

$$(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B_{k'}}{k'} \pmod{p^{N+1}}.$$

(3) *Если* $(p-1)\mid k$ *и* k *четно* (*или* $k=1$, $p=2$), *то*

$$pB_k \equiv -1 \pmod{p}.$$

Доказательство. Предположим, что $p>2$. Доказательство утверждения (3) при $p=2$ мы оставляем читателю в качестве упражнения (см. ниже упр. 6).

Сейчас нам понадобится один факт, доказательство которого будет дано ниже, в начале следующей главы (см. конец § III.1): существует такое $\alpha \in \{2, 3, \ldots, p-1\}$, что α^{p-1} есть степень числа α с наименьшим положительным показателем, сравнимая с 1 по модулю p. Иначе говоря, мультипликативная группа ненулевых классов вычетов кольца $\mathbb{Z}$ по модулю p является циклической группой порядка $p-1$, т. е. существует образующая $\alpha \in \{2, 3, \ldots, p-1\}$, для

которой наименьшие положительные вычеты элементов α, α^2, α^3, ..., α^{p-1} исчерпывают все множество $\{1, 2, 3, \ldots, p-1\}$.

При доказательстве утверждений (1) и (2) в качестве «регуляризатора меры» α берется такая образующая из $\{2, 3, \ldots, p-1\}$. Поэтому, так как $(p-1) \nmid (-k)$, то $\alpha^{-k} \not\equiv 1 \pmod{p}$ и $(\alpha^{-k}-1)^{-1} \in \mathbb{Z}_p^\times$.

Докажем теперь (1) (предполагая, что $k > 1$; если $k = 1$ и $p > 2$, то $|B_1/1|_p = |-1/2|_p = 1$). Имеем

$$|B_k/k|_p = \left|\frac{1}{\alpha^{-k}-1}\right|_p \left|\frac{1}{1-p^{k-1}}\right|_p \left|\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}\right|_p =$$

$$= \left|\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}\right|_p \leqslant 1,$$

по предложению в конце § 5 (с $A = B = 1$), так как $|\mu_{1,\alpha}(U)|_p \leqslant 1$ для любого компактно-открытого подмножества $U \subset \mathbb{Z}_p^\times$ и $|x^{k-1}|_p \leqslant 1$ для всех $x \in \mathbb{Z}_p^\times$.

Чтобы доказать (2), запишем требуемое сравнение в виде

$$\frac{1}{\alpha^{-k}-1}\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha} \equiv \frac{1}{\alpha^{-k'}-1}\int_{\mathbb{Z}_p^\times} x^{k'-1}\mu_{1,\alpha} \pmod{p^{N+1}}.$$

Заметим, что если для некоторых a, b, c, $d \in \mathbb{Z}_p$ выполнены сравнения $a \equiv c \pmod{p^n}$ и $b \equiv d \pmod{p^n}$, то $ab \equiv cb \equiv cd \pmod{p^n}$. Таким образом, поскольку $a = (\alpha^{-k}-1)^{-1}$, $b = \int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}$, $c = (\alpha^{-k'}-1)^{-1}$, $d = \int_{\mathbb{Z}_p^\times} x^{k'-1}\mu_{1,\alpha}$ принадлежат $\mathbb{Z}_p$, достаточно установить сравнения $(\alpha^{-k}-1)^{-1} \equiv (\alpha^{-k'}-1)^{-1} \pmod{p^{N+1}}$ и $\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha} \equiv \int_{\mathbb{Z}_p^\times} x^{k'-1}\mu_{1,\alpha} \pmod{p^{N+1}}$. Первое из них сводится к $\alpha^k \equiv \alpha^{k'} \pmod{p^{N+1}}$, а второе (согласно следствию в конце § 5 с $B = 1$ и $\varepsilon = p^{-N-1}$) — к $x^{k-1} \equiv x^{k'-1} \pmod{p^{N+1}}$ для любых $x \in \mathbb{Z}_p^\times$. Оба эти факта нетрудно получить из рассуждений § 2.

В заключение докажем сравнение Клаузена — фон Штаудта. Для этого рассмотрим $\alpha = 1 + p$. Напомним,

что мы ограничились случаем $p>2$. Итак,

$$pB_k = -kp(-B_k/k) = \frac{-kp}{\alpha^{-k}-1}\frac{1}{1-p^{k-1}}\int\limits_{Z_p^\times} x^{k-1}\mu_{\alpha,1}.$$

Вначале возьмем первый из трех сомножителей справа. Если $d=\operatorname{ord}_p k$, то $\alpha^{-k}-1=(1+p)^{-k}-1\equiv \equiv -kp \pmod{p^{d+2}}$, откуда

$$1\equiv \frac{-kp}{\alpha^{-k}-1} \pmod p.$$

Далее, так как $k\geqslant 2$, имеем $(1-p^{k-1})^{-1}\equiv 1 \pmod p$. Следовательно,

$$pB_k \equiv \int\limits_{Z_p^\times} x^{k-1}\mu_{1,\alpha} \pmod p.$$

Используя снова следствие в конце § 5, на этот раз для функций $f(x)=x^{k-1}$ и $g(x)=1/x$, мы получаем

$$pB_k \equiv \int\limits_{Z_p^\times} x^{-1}\mu_{1,\alpha} \pmod p.$$

Последний интеграл сравним с -1 по модулю p в силу упр. 7 к § 5. □

Вернемся теперь к p-адической интерполяции.

Определение. Фиксируем некоторое $s_0\in\{0, 1, 2, \ldots, p-2\}$. Для $s\in\mathbb{Z}_p$ ($s\neq 0$, если $s_0=0$) положим

$$\zeta_{p,s_0}(s) \underset{\text{def}}{=} \frac{1}{\alpha^{-(s_0+(p-1)s)}-1}\int\limits_{Z_p^\times} x^{s_0+(p-1)s-1}\mu_{1,\alpha}.$$

Смысл этого определения сейчас должен быть ясен: значения

$$\alpha^{-(s_0+(p-1)s)} = \alpha^{-s_0}(\alpha^{p-1})^{-s} \quad \text{и}$$
$$x^{s_0+(p-1)s-1} = x^{s_0-1}(x^{p-1})^s$$

для любого $x\in\mathbb{Z}_p^\times$ и целого p-адического s определяются как пределы соответствующих значений для последовательности целых положительных чисел $\{k_i\}$, p-адически стремящейся к s. Значение $\zeta_{p,s_0}(s)$ можно

также определить как предел

$$-\lim_{k_i \to s} \left(1 - p^{s_0 + (p-1)k_i - 1}\right) B_{s_0 + (p-1)k_i}/(s_0 + (p-1)k_i).$$

Теперь очевидно, что для каждого целого положительного k, сравнимого с s_0 по модулю $p-1$, т. е. $k = s_0 + (p-1)k_0$, мы имеем $\zeta_p(1-k) = \zeta_{p, s_0}(k_0)$. Поэтому функции ζ_{p, s_0} можно рассматривать как p-адические «ветви» функции ζ_p — одна ветвь для каждого класса вычетов по модулю $p-1$. (Отметим, что нечетным классам вычетов $s_0 = 1, 3, \ldots, p-2$ отвечает нулевая функция, так как $B_{s_0 + (p-1)k_i} = 0$ для таких s_0; по этой причине интересны только четные s_0.)

В определении ζ_{p, s_0} значение $s = 0$ при $s_0 = 0$ исключено. Причина этого в том, что при $s = 0$ было бы $\alpha^{-(s_0 + (p-1)s)} = 1$, так что знаменатель в определении функции обратился бы в нуль. Как видно из записи $\zeta_p(1-k) = \zeta_{p, s_0}(k_0)$, где $k = s_0 + (p-1)k_0$, исключенный случай соответствует значению $\zeta_p(1)$. Таким образом, p-адическая дзета-функция, подобно архимедовой дзета-функции Римана, обладает «полюсом» в 1.

Теорема 8. *Фиксируем простое p и некоторый вычет s_0. Тогда функция $\zeta_{p, s_0}(s)$ ($s \neq 0$ при $s_0 = 0$) является непрерывной функцией p-адического аргумента s и ее определение не зависит от выбора $\alpha \in \mathbb{Z}$, $p \nmid \alpha$, $\alpha \neq 1$.*

Доказательство. Непрерывность по s интеграла в определении функции получается непосредственно из рассуждений § 2 и следствия в конце § 5. Множитель $1/(\alpha^{-(s_0 + (p-1)s)} - 1)$ непрерывен, если при $s_0 = 0$ исключить значение $s = 0$, потому что непрерывна функция $\alpha^{-(s_0 + (p-1)s)}$ (согласно § 2). Поэтому $\zeta_{p, s_0}(s)$ также непрерывна.

Остается установить независимость $\zeta_{p, s_0}(s)$ от α. Пусть $\beta \in \mathbb{Z}$, $p \nmid \beta$, $\beta \neq 1$. Две функции

$$\frac{1}{\alpha^{-(s_0 + (p-1)s)} - 1} \int_{\mathbb{Z}_p^\times} x^{s_0 + (p-1)s - 1} \mu_{1, \alpha},$$

$$\frac{1}{\beta^{-(s_0 + (p-1)s)} - 1} \int_{\mathbb{Z}_p^\times} x^{s_0 + (p-1)s - 1} \mu_{1, \beta}$$

совпадают для любых целых $s_0+(p-1)s=k$, бо́льших 0, т. е. для любых целых неотрицательных s ($s>0$ при $s_0=0$), поскольку в этом случае обе данные функции принимают одно и то же значение $(1-p^{k-1})\times$ $\times(-B_k/k)$. Но множество целых неотрицательных чисел плотно в $\mathbb{Z}_p$, поэтому любые две непрерывные функции, совпадающие на этом множестве, равны. Следовательно, замена α на β не влияет на определение $\zeta_{p,\,s_0}$. □

Теорема 8 дает p-адическую интерполяцию «интересной части» $-B_{2k}/2k$ значений $\zeta(2k)$. Осталось только объяснить несколько вещей: (1) термин «преобразование Меллина — Мазура» в названии этого параграфа и (2) таинственную замену k на $1-k$. Кроме того, следует сказать кое-что о (3) более глубокой аналогии с классическими ζ-функциями и L-функциями, а также о (4) связи с модулярными формами. Так как эти четыре темы вывели бы нас далеко за рамки материала, отобранного для изложения с доказательствами в этой книге, то ниже мы лишь вкратце расскажем о самых основных фактах, сюда относящихся. Доказательства и дальнейшие сведения по темам (1) — (4) можно найти в следующих работах: (1) Манин [(c) 6], § 8; (2) Ивасава [(c) 1], § 1 и приложение; (3) Ивасава [(c) 1], особенно § 5, Боревич и Шафаревич [(b) 1], стр. 439—444; (4) Серр [(c) 5].

§ 7. КРАТКИЙ ОБЗОР (БЕЗ ДОКАЗАТЕЛЬСТВ)

(1) Функция $\zeta(s)$ при $s>1$ представима в виде интеграла

$$\frac{1}{\Gamma(s)}\int_0^\infty x^{s-1}\frac{dx}{e^x-1},$$

где $\Gamma(s)$ — гамма-функция, которая удовлетворяет функциональному уравнению $\Gamma(s+1)=s\Gamma(s)$, а $\Gamma(1)=1$, откуда $\Gamma(k)=(k-1)!$ для всех целых положительных k. (Случай $s=k$ см. ниже в упр. 4.) Этот интеграл известен как преобразование Меллина. Вообще, если

$f(x)$ — некоторая функция, определенная на множестве положительных вещественных чисел, то функция

$$g(s)=\int_0^\infty x^{s-1}f(x)\,dx$$

всякий раз, когда она определена, называется преобразованием Меллина функции $f(x)$ (или дифференциальной формы $f(x)\,dx$). Таким образом, $\Gamma(s)\zeta(s)$ есть преобразование Меллина дифференциала $dx/(e^x-1)$, определенное при $s>1$ (см. ниже упр. 4).

В § 6 было показано, что функция, p-адически интерполирующая $(1-p^{k-1})(-B_k/k)$, совпадает по существу (с точностью до множителя $1/(\alpha^{-s}-1)$ и некоторого изменения аргумента в соответствии с выбором s_0) с интегралом

$$\int_{\mathbf{Z}_p^\times} x^{s-1}\mu_{1,\alpha},$$

где $\mu_{1,\alpha}$ — регуляризованная мера Мазура. Следовательно, подобно классической дзета-функции, p-адическую ζ-функцию можно рассматривать как «p-адическое преобразование Меллина — Мазура» регуляризованной меры Мазура $\mu_{1,\alpha}$.

(2) Рассмотрим ряд

$$\zeta(s)=\sum_{n=1}^\infty \frac{1}{n^s}$$

для комплексных значений s с вещественной частью >1. Этот ряд сходится и определяет в этой области значений s комплексно аналитическую функцию. Эта функция $\zeta(s)$ допускает *аналитическое продолжение* на всю комплексную плоскость, за исключением точки $s=1$ (в окрестности которой она ведет себя как $1/(s-1)$). Фундаментальное свойство $\zeta(s)$ заключается в том, что она удовлетворяет *функциональному уравнению*, связывающему ее значения в точках s и $1-s$, а именно:

$$\zeta(1-s)=\frac{2\cos(\pi s/2)\,\Gamma(s)}{(2\pi)^s}\zeta(s).$$

Пусть $s = 2k$ — целое четное положительное число. Тогда

$$\zeta(1-2k) = \frac{2\cos \pi k\,(2k-1)!}{(2\pi)^{2k}}\,\zeta(2k) =$$

$$= \frac{2(-1)^k(2k-1)!}{(2\pi)^{2k}}\,\frac{(-1)^k\pi^{2k}2^{2k-1}}{(2k-1)!}\left(-\frac{B_{2k}}{2k}\right) = -\frac{B_{2k}}{2k}$$

(по теореме 4). С другой стороны, если s — *нечетное* целое число > 1, то правая часть функционального уравнения обращается в нуль, так как $\cos(\pi s/2) = 0$ (предположение $s > 1$ необходимо для конечности $\zeta(s)$). Следовательно, $\zeta(1-s)$ равно нулю, что также согласуется с формулой $\zeta(1-k) = -B_k/k$. Иначе говоря, функциональное уравнение в этом случае утверждает, что $0 = 0$.

Вот несколько первых значений $\zeta(1-k) = -B_k/k$:

$1-k$	-1	-3	-5	-7	-9	-11	-13	-15	-17	-19	-21
$\zeta(1-k)$	$-\frac{1}{12}$	$\frac{1}{120}$	$-\frac{1}{252}$	$\frac{1}{240}$	$-\frac{1}{132}$	$-\frac{691}{32760}$	$-\frac{1}{12}$	$\frac{3617}{8160}$	$-\frac{43867}{14364}$	$\frac{174611}{6600}$	$-\frac{77683}{276}$

Поэтому «в действительности» мы интерполировали ζ-функцию Римана, заданную на множестве *целых отрицательных нечетных чисел*. Следующее соотношение устанавливает простую связь между ζ_p и ζ:

$$\zeta_p(1-k) = (1-p^{k-1})\,\zeta(1-k), \quad k = 2,\ 3,\ 4,\ \ldots\ .$$

Пренебрегая всеми расходимостями, можно написать $\zeta(1-k) = \prod_{\text{простые } q} 1/(1-q^{k-1})$, откуда

$$\zeta^*(1-k) = \prod_{\text{простые } q,\ q\neq p} 1/(1-q^{k-1}) = (1-p^{k-1})\,\zeta(1-k).$$

Появление множителя $1-p^{k-1}$ становится эвристически понятным с этой «беззаботной» точки зрения.

В том же стиле можно непосредственно вывести формулу $\zeta(1-k) = -B_k/k$:

$$\zeta(1-k) \overset{\text{def}}{=} \sum_{n=1}^{\infty} \frac{1}{n^{1-k}} = \sum_{n=1}^{\infty} n^{k-1}.$$

Так как $(d/dt)^{k-1}e^{nt}|_{t=0} = n^{k-1}$, то

$$\zeta(1-k) = \sum_{n=1}^{\infty} \left(\frac{d}{dt}\right)^{k-1} e^{nt}\Big|_{t=0} = \left(\frac{d}{dt}\right)^{k-1} \sum_{n=1}^{\infty} e^{nt}\Big|_{t=0} =$$

$$= \left(\frac{d}{dt}\right)^{k-1} \left(\frac{1}{1-e^t} - 1\right)\Big|_{t=0} = \left(\frac{d}{dt}\right)^{k-1} \left(\frac{1}{1-e^t}\right)\Big|_{t=0} =$$

$$= \left(\frac{d}{dt}\right)^{k-1} \left(-\frac{1}{t} \sum_{n=1}^{\infty} B_n \frac{t^n}{n!}\right)\Big|_{t=0} =$$

$$= \left(\frac{d}{dt}\right)^{k-1} \sum \left(-\frac{B_n}{n}\right) \frac{t^{n-1}}{(n-1)!}\Big|_{t=0} = -\frac{B_k}{k}.$$

(3) Существуют и более глубокие связи между ζ_p и ζ. Один важный пример такой связи требует введения функций следующего вида:

$$L_\chi(s) \underset{\text{def}}{=} \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad s>0,$$

обобщающих ζ-функцию; здесь χ — некоторый *характер Дирихле* (см. упр. 9—10 к § 2). Если характер χ *не тривиален* (т. е. отличен от 1 для некоторого n), то функция $L_\chi(s)$ сходится при $s=1$. Более того, имеет место явная формула

$$L_\chi(1) = -\frac{\tau(\chi)}{N} \sum_{a=1}^{N-1} \bar{\chi}(a) \log(1 - e^{-2\pi i a/N}),$$

где N — кондуктор характера χ, а $\tau(\chi) = \sum_{a=1}^{N-1} \chi(a) e^{2\pi i a/N}$

(эта формула легко приводится к виду, указанному в упр. 9—10 к § 2).

Функция $L_\chi(1-k)$ допускает p-адическую интерполяцию; конструкция, аналогичная конструкции ζ_p, позволяет построить *p-адическую L-функцию* $L_{\chi,p}$. Неожиданно оказывается, что значение $L_{\chi,p}(1)$ равно следующему выражению:

$$-\left(1 - \frac{\chi(p)}{p}\right) \frac{\tau(x)}{N} \sum_{a=1}^{N-1} \bar{\chi}(a) \log_p(1 - e^{-2\pi i a/N}),$$

в котором $\log_p$ обозначает «*p-адический логарифм*», являющийся p-адической функцией от p-адического аргумента (см. § IV.1 и упр. 5 к § IV.2), и все встречающиеся в данном выражении корни из единицы, а именно $e^{2\pi ia/N}$ и значения характера χ, рассматриваются как элементы алгебраического расширения поля $\mathbb{Q}_p$ (см. § III. 2—3). Множитель $1-\chi(p)/p$ нужно представлять себе как p-множитель Эйлера (для обычной ζ-функции $\chi=1$ и множитель Эйлера для $\zeta(1)$, будь это значение конечным, был бы равен $1-1/p$; см. также часть упр. 9 к § 2, касающуюся эйлеровых произведений для L_χ). В остальном выражение для $L_{\chi,p}(1)$ совпадает с явной формулой для $L_\chi(1)$, за тем исключением, что в этой формуле классический log заменен его p-адическим аналогом $\log_p$.

(4) Важную роль при изучении эллиптических кривых и модулярных форм (см. Серр [(b) 3], гл. VII) играют ряды Эйзенштейна E_{2k}, $k\geqslant 2$, которые представляют собой функции, определенные для всех комплексных чисел z с положительной мнимой частью следующим образом:

$$E_{2k}(z)=-\frac{1}{2}\frac{B_{2k}}{2k}+\sum_{n=1}^{\infty}\sigma_{2k-1}(n)\,e^{2\pi inz},$$

где

$$\sigma_m(n)\underset{\text{def}}{=}\sum_{d\mid n}d^m.$$

Каждый такой ряд есть ряд Фурье, т. е. некоторый степенной ряд относительно $e^{2\pi iz}$, с постоянным членом $\frac{1}{2}\zeta(1-2k)$.

Оказывается, ряды Эйзенштейна допускают p-адическую интерполяцию. На это указывает, в частности, p-адическая интерполируемость n-го коэффициента, если только $p\nmid n$. Действительно, каждый такой коэффициент $\sigma_{2k-1}(n)$ равен конечной сумме значений функций d^{2k-1}, которые интерполируются согласно результатам § 2 при $p\nmid d$. Тогда интерполяцию $\zeta(1-2k)$ можно рассматривать как «вычисление нулевого коэффициента». Как бы туманно это ни выглядело, в действительности все результаты этой главы можно извлечь из теории

p-адических модулярных форм. Подробности см. в упомянутой выше статье Серра, а также в серии статей Н. Катца по p-адическим мерам Эйзенштейна и p-адической интерполяции рядов Эйзенштейна (см. литературу).

Упражнения

1. Используя соотношения между $\mu_{1,\alpha}$, $\mu_{k,\alpha}$ и $\mu_{B,k}$, докажите непосредственно (без упоминания чисел Бернулли) независимость от α выражения

$$\frac{1}{\alpha^{-k}-1}\int_{\mathbb{Z}_p^\times} x^{k-1}\mu_{1,\alpha}.$$

2. Пользуясь таблицей значений $\zeta(1-k)$, проверьте сравнения Куммера для $p=5$, $k=2$, $k'=22$, $N=1$. Также по этой таблице проверьте, что эти сравнения неверны, если $(p-1)\nmid k$. Используя сравнения Куммера и несколько первых чисел B_k, вычислите следующие числа по модулю p^2:

(i) B_{102} в $\mathbb{Q}_5$; (ii) B_{206} в $\mathbb{Q}_7$; (iii) B_{502} в $\mathbb{Q}_7$.

3. Применяя теорему 7 и упр. 19 к § I.2, докажите следующий вариант теоремы Клаузена—фон Штаудта: $(B_k+\sum 1/p)\in\mathbb{Z}$, где суммирование производится по всем p, для которых $(p-1)\mid k$.

4. Установите существование интеграла $\int_0^\infty x^{s-1}\,dx/(e^x-1)$ при $s>1$. Записав $1/(e^x-1)=e^{-x}/(1-e^{-x})=\sum_{n=1}^{\infty} e^{-nx}$, покажите, что

$$\int_0^\infty \frac{x^{k-1}}{e^x-1}\,dx=(k-1)!\,\zeta(k),\qquad k=2,\ 3,\ 4,\ \ldots$$

(представьте обоснования ваших вычислений).

5. Докажите, что

$$\int_0^\infty \frac{x^{k-1}}{e^x+1}\,dx=(k-1)!\,(1-2^{1-k})\,\zeta(k)$$

для $k=2, 3, 4, \ldots$. Покажите, что функция

$$\frac{1}{\Gamma(s)(1-2^{1-s})}\int_0^\infty \frac{x^{s-1}}{e^x+1}\,dx,$$

которая, как вы только что доказали, совпадает с $\zeta(s)$ при $s=k=2, 3, 4, \ldots$, определена и непрерывна на множестве чисел $s>0$, $s\neq 1$.

6. Докажите теорему Клаузена—фон Штаудта для $p=2$. (*Указание.* Возьмите $\alpha=1+p^2=5$ и $g(x)=(a_0+2a_1)^{-1}$, где a_0, a_1 — два первых 2-адических знака x.) Скажите словами, что утверждает эта теорема о числителе и знаменателе числа B_k при четном k и $p=2$.

Глава III

КОНСТРУКЦИЯ ПОЛЯ Ω

§ 1. КОНЕЧНЫЕ ПОЛЯ

В дальнейшем нам придется предполагать, что читатель знаком с основными понятиями, касающимися алгебраических расширений полей. Повторение всех необходимых доказательств увело бы нас далеко в сторону. Достаточно полное и доступное изложение можно найти в книге Ленга [(a) 3] или Херстейна [(a) 2]. Нам понадобятся следующие понятия и факты.

(1) Абстрактное определение *поля* F; под *расширением* K поля F понимается произвольное поле K, содержащее F в качестве подполя; расширение K называется *алгебраическим,* если любой элемент $\alpha \in K$ является корнем некоторого многочлена с коэффициентами в F: $a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n = 0$, где $a_i \in F$. Например, множество чисел вида $a + b\sqrt{2}$ с $a,\ b \in \mathbb{Q}$ представляет собой алгебраическое расширение поля $\mathbb{Q}$.

(2) Пусть F — некоторое поле. Наименьшее целое положительное число n, для которого 1, будучи сложена сама с собой n раз, дает в результате 0, называется *характеристикой* поля F и обозначается через $\mathrm{char}\,(F)$. Если $1 + 1 + \ldots + 1$ всегда $\neq 0$, то по определению $\mathrm{char}\,(F) = 0$. (Логичнее было бы полагать $\mathrm{char}\,(F) = \infty$, однако принято считать характеристику поля в этом случае равной 0.) Поля $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{R}$ и $\mathbb{C}$ имеют характеристику 0, тогда как множество классов вычетов кольца $\mathbb{Z}$ по простому модулю p является полем характеристики p. (Вскоре нам встретятся другие примеры полей характеристики p.)

(3) Определение *векторного пространства* V над полем F; понятие *базиса* V над F; свойство *конечномерности* векторного пространства V; если V конечно-

мерно, то его *размерность* равна числу элементов любого базиса.

(4) Любое расширение K поля F можно рассматривать как векторное пространство над F; если это пространство конечномерно, то соответствующее расширение будет алгебраическим; размерность этого векторного пространства называется *степенью* расширения и обозначается $[K:F]$. Если $\alpha \in K$ обладает тем свойством, что каждый элемент поля K представим в виде рационального выражения от α над F, то говорят, что расширение K получено *присоединением* элемента α к полю F, и записывают это в виде $K = F(\alpha)$. Пусть K' — конечное расширение поля K. Тогда легко установить конечность K' как расширения поля F и соотношение $[K':F] = [K':K] \cdot [K:F]$.

(5) Пусть α — элемент алгебраического расширения K поля F. Тогда существует *единственный* неприводимый многочлен со старшим коэффициентом 1 (*неприводимость* означает, что его нельзя разложить в произведение многочленов меньшей степени с коэффициентами в F), такой, что

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0, \quad a_i \in F.$$

Этот многочлен называется *минимальным многочленом* элемента α, а число n — *степенью* данного элемента α. Расширение $F(\alpha)$ имеет степень n над F (действительно, в качестве базиса векторного пространства $F(\alpha)$ над F можно взять набор элементов $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$).

(6) Если поле F имеет характеристику 0 (например, $\mathbb{Q}$ или $\mathbb{Q}_p$) или является конечным (подробное изложение теории конечных полей следует за данным обзором), то можно доказать, что каждое конечное расширение K поля F имеет вид $K = F(\alpha)$ для некоторого $\alpha \in K$. Такой элемент α называется *примитивным*. (На самом деле это верно, если поле F *совершенное*, т. е. либо $\mathrm{char}(F) = 0$, либо $\mathrm{char}(F) = p$ и каждый элемент поля F обладает корнем степени p в F.) Знание примитивного элемента α расширения K упрощает изучение этого K, так как в этом случае каждый эле-

мент из K представим в виде многочлена от α степени $<n$, т. е. $K=\left\{\sum_{i=0}^{n-1} a_i\alpha^i \mid a_i\in F\right\}$.

(7) Рассмотрим некоторый неприводимый многочлен f степени n с коэффициентами в F. Можно построить расширение $K\supset F$ степени n, в котором f имеет корень $\alpha\in K$. Последовательно присоединяя корни всех многочленов с коэффициентами в F, мы получаем *алгебраическое замыкание* (обозначаемое $F^{\mathrm{al;\ cl}}$ или $\bar{F}$) поля F, т. е., по определению, наименьшее алгебраически замкнутое поле, содержащее F (напомним, что поле K называется *алгебраически замкнутым*, если всякий многочлен с коэффициентами в K имеет корень в K). Всякое алгебраическое расширение поля F содержится в некотором его алгебраическом замыкании (т. е. его можно расширить до алгебраического замыкания поля F). Любые два алгебраических замыкания поля F изоморфны. Поэтому мы обычно пишем «алгебраическое замыкание» вместо «любое алгебраическое замыкание». Как правило, алгебраическое замыкание поля F является объединением бесконечного множества конечных алгебраических расширений поля F. Так, например, алгебраическое замыкание поля $\mathbb{Q}$ состоит из всех комплексных чисел, являющихся корнями многочленов с рациональными коэффициентами. Однако алгебраическое замыкание поля вещественных чисел $\mathbb{R}$ равно $\mathbb{C}=\mathbb{R}(\sqrt{-1})$, т. е. это конечное расширение степени 2 поля $\mathbb{R}$. Но этот пример — скорее исключение, чем правило.

(8) Пусть $K=F(\alpha)$, K' — другое расширение поля F, а $\sigma: K\to K'$ — изоморфное вложение поля K в K' (где σ — некоторый F-гомоморфизм, т. е. это отображение сохраняет все операции поля и $\sigma(a)=a$ для любого $a\in F$). Тогда элемент α и его образ $\sigma(\alpha)$ в K' обладают одним и тем же минимальным многочленом. Обратно, пусть $K=F(\alpha)$, K' — другое расширение поля F и $\alpha'\in K'$ — корень минимального многочлена для α. Тогда существует единственный изоморфизм σ поля K на подполе $F(\alpha')\subset K'$, для которого $\sigma(a)=a$ при любом $a\in F$ и $\sigma(\alpha)=\alpha'$.

(9) Все корни минимального многочлена над F элемента $\alpha \in \bar{F}$, лежащие в поле $\bar{F} = F^{\text{alg cl}}$, называются элементами, *сопряженными* с α. Существует взаимно однозначное соответствие между изоморфными вложениями $F(\alpha)$ в $\bar{F}$ и элементами α', сопряженными с α (см. предыдущий пункт (8)). Если $\operatorname{char}(F) = 0$ или F — конечное поле (или F — совершенное поле), то каждый неприводимый многочлен с коэффициентами в F не имеет кратных корней. В этом случае число элементов, сопряженных с α, равно $[F(\alpha) : F]$.

(10) Расширение $K = F(\alpha)$ поля F называется *расширением Галуа*, если все элементы, сопряженные с α, лежат в K. В этом случае все сопряженные любого элемента $x = \sum_{i=0}^{n-1} a_i \alpha^i \in K$ также лежат в K, поскольку такие сопряженные имеют вид $\sum_{i=0}^{n-1} a_i \alpha'^i$, где α' — элемент, сопряженный с α. Приведем несколько примеров расширений Галуа поля $\mathbb{Q}$: $\mathbb{Q}(\sqrt{2})$ (так как $\alpha = \sqrt{2}$ обладает единственным сопряженным, равным другому корню $\alpha' = -\sqrt{2}$ уравнения $x^2 - 2 = 0$, и $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$); $\mathbb{Q}(i)$; $\mathbb{Q}(\sqrt{d})$ для любого $d \in \mathbb{Q}$; $\mathbb{Q}(\zeta_m)$, где $\zeta_m = e^{2\pi i/m}$ — примитивный корень из 1 степени m, лежащий в $\mathbb{C}$ (так как все сопряженные с ζ_m — это другие примитивные корни степени m, а они имеют вид ζ^i_m, где i взаимно просто с m). Поле $\mathbb{Q}(\sqrt[4]{2})$ дает пример расширения поля $\mathbb{Q}$, которое не есть расширение Галуа. Действительно, сопряженные с $\sqrt[4]{2}$ — это 4 корня уравнения $x^4 - 2 = 0$, а именно: $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$. Но $i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$ (так как $\mathbb{Q}(\sqrt[4]{2})$ содержится в поле вещественных чисел).

(11) Пусть K — некоторое расширение Галуа поля F. Тогда образ каждого изоморфизма из пункта (8) совпадает с K, т. е. все эти изоморфизмы являются F-изоморфизмами поля K в себя, или *F-автоморфизмами* поля K. Эти автоморфизмы образуют группу, которая называется *группой Галуа поля K над F*. Каждый автоморфизм σ из этой группы определяет множество

элементов $x \in K$, для которых $\sigma(x) = x$. Оно называется *полем σ-инвариантов* (легко проверить, что это действительно подполе в K, содержащее F). Рассмотрим следующий пример: поле $K = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ — расширение Галуа поля $\mathbb{Q}$ степени 4; возьмем автоморфизм σ, переводящий $\sqrt{2}+\sqrt{3}$ в $\sqrt{2}-\sqrt{3}$; тогда поле σ-инвариантов совпадает с $\mathbb{Q}(\sqrt{2})$. Нетрудно установить, что если K — расширение Галуа поля F, а $K' \neq K$ — некоторое промежуточное поле между K и F: $F \subset K' \subset K$, то существует нетривиальный автоморфизм поля K, оставляющий неподвижными все элементы из K'. Более того, существует взаимно однозначное соответствие между подгруппами S группы Галуа поля K над F и промежуточными полями $F \subset K' \subset K$, такое, что

$$S \leftrightarrow K'_S = \{x \in K \mid \sigma x = x \text{ для любого } \sigma \in S\}.$$

Однако в дальнейшем теория Галуа не понадобится нам во всей своей силе; мы будем опираться лишь на некоторые частные случаи сформулированных здесь результатов.

Перейдем теперь к изучению конечных полей. Простейший пример такого поля есть поле *классов вычетов целых чисел по простому модулю p*. Элементами этого поля являются классы эквивалентности целых чисел по отношению эквивалентности $x \sim y$, определяемому как $x \equiv y \pmod{p}$. Существует ровно p таких классов эквивалентности, а именно классы элементов $0, 1, 2, 3, \ldots, p-2, p-1$. На множестве этих классов легко ввести операции сложения и умножения, а затем проверить, что при этом получится поле (в частности, каждый ненулевой класс эквивалентности обратим по умножению; иначе говоря, если x — целое, не делящееся на p, то существует целое y, для которого $xy \equiv 1 \pmod{p}$). Это поле обозначается $\mathbb{F}_p$, а иногда $\mathbb{Z}/p\mathbb{Z}$ (*факторкольцо кольца целых чисел по идеалу целых чисел, делящихся на p*). С таким же успехом можно построить это поле, исходя из множества целых p-адических чисел $\mathbb{Z}_p$ и отношения эквивалентности $x \sim y$ ($x, y \in \mathbb{Z}_p$), определяемого как $x \equiv y \pmod{p}$ (т. е. эквивалентные x и y

имеют один и тот же первый знак в p-адическом разложении). Поэтому поле $\mathbb{F}_p$ можно записывать также в виде $\mathbb{Z}_p/p\mathbb{Z}_p$ (*факторкольцо кольца целых p-адических чисел по идеалу p-адических целых, делящихся на p.*) Факторкольцо $\mathbb{Z}_p/p\mathbb{Z}_p$ называется *полем вычетов* кольца $\mathbb{Z}_p$. Причина нашего интереса к общим конечным полям заключается в том, что ниже, при исследовании алгебраических расширений поля $\mathbb{Q}_p$, мы столкнемся с их полями вычетов, которые строятся аналогично полю вычетов для $\mathbb{Z}_p \subset \mathbb{Q}_p$, однако оказываются уже совсем не такими простыми, как $\mathbb{F}_p$. Они представляют собой алгебраические расширения поля $\mathbb{F}_p$. Поэтому сейчас нам необходимо получить некоторое представление о том, как же выглядят конечные поля вообще.

Пусть F — конечное поле. Тогда характеристика $F \neq 0$, так как все элементы $0, 1, 1+1, 1+1+1, \ldots$ из F не могут быть различными. Пусть $n = \mathrm{char}\,(F)$. Заметим, что число n должно быть простым. Действительно, если $n = n_0 n_1$ для n_0 и $n_1 < n$, то $n_0 \neq 0$ и после умножения на n_0^{-1} мы получаем противоречие: $n_1 = n_0^{-1} n = 0$. Обозначим это простое число $\mathrm{char}\,(F)$ через p.

Очевидно, любое поле F характеристики p содержит в качестве подполя описанное выше поле из p элементов (оно состоит из элементов вида $1+1+\ldots+1$). Это подполе называется *простым подполем* в F.

Заметим теперь, что для каждого поля F характеристики p определено отображение $x \longmapsto x^p$, сохраняющее операции сложения и умножения:

$$xy \longmapsto (xy)^p = x^p y^p,$$

$$x + y \longmapsto (x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p,$$

потому что целое число $\binom{p}{i} = p!/i!\,(p-i)!$ делится на p при $1 \leqslant i \leqslant p-1$, а поэтому соответствующий элемент в F равен 0.

Теорема 9. *Пусть F — конечное поле, состоящее из q элементов, а $f = [F : \mathbb{F}_p]$ (размерность F как векторного пространства над своим простым подполем $\mathbb{F}_p$). Обозначим через K некоторое алгебраическое замыкание поля $\mathbb{F}_p$, содержащее F. Тогда $q = p^f$; F — единственное под-*

поле в K, состоящее из q элементов; при этом F есть множество всех элементов из K, удовлетворяющих уравнению $x^q - x = 0$. Обратно, для каждой степени $q = p^f$ простого p корни уравнения $x^q - x = 0$ задают подполе из q элементов в K.

Доказательство. Так как F является f-мерным векторным пространством над $\mathbb{F}_p$, число элементов этого пространства равно числу всевозможных выборов значений для f компонент вектора (т. е. *координат* в некотором базисе, состоящем из f элементов) в $\mathbb{F}_p$, а поэтому равно p^f. Далее, каждое поле F из q элементов содержит $q-1$ ненулевых элементов. Эти ненулевые элементы из F образуют мультипликативную группу порядка $q-1$. Степени любого элемента $x \neq 0$ составляют подгруппу этой группы. Порядок ее равен показателю наименьшей степени x, равной 1 (этот показатель называется также *порядком* элемента x). Легко доказать, что порядок любой подгруппы конечной группы делит порядок всей группы. Следовательно, порядок x делит $q-1$, откуда $x^{q-1} = 1$ для любого ненулевого x из F. Поэтому $x^q - x = 0$ для любого x (включая 0) из F. Последнее справедливо для *каждого* подполя из q элементов в K. Кроме того, всякий многочлен степени q имеет в любом поле не более чем q различных корней. Из этого следует, что каждое поле из q элементов в K должно состоять из корней многочлена $x^q - x$, а такое множество единственно.

Обратно, пусть $q = p^f$. Тогда множество элементов поля K, для которых $x^q = x$, замкнуто относительно сложения и умножения (это доказывается так же, как и утверждение, предшествующее формулировке теоремы). Итак, это подполе поля K. Многочлен $x^q - x$ не имеет кратных корней. Действительно, в противном случае из упр. 10 ниже следовало бы, что кратный корень является также корнем формальной производной этого многочлена $qx^{q-1} - 1 = -1$ (так как $q = 0$ в K). Но многочлен -1 не имеет корней. □

Замечание. Поскольку любые два алгебраических замыкания поля $\mathbb{F}_p$ изоморфны, изоморфны также любые два поля, состоящие из $q = p^f$ элементов.

Обозначим через $\mathbb{F}_q$ единственное (с точностью до изоморфизма) поле из $q = p^l$ элементов.

Если F — некоторое поле, то через $F^\times$ обозначается группа его ненулевых элементов.

Предложение. *Группа $\mathbb{F}_q^\times$ является циклической группой порядка $q-1$.*

Доказательство. Пусть $o(x)$ обозначает порядок элемента x (наименьший показатель степени x, равной 1). Нам уже известно, что $o(x)$ делит $q-1$ при любом $x \in \mathbb{F}_q^\times$. Однако если d — делитель $q-1$, то уравнение $x^d = 1$ имеет не более чем d решений, потому что всякий полином степени d имеет в любом поле не более чем d корней. Следовательно, если $d = o(x)$, то d различных элементов $x, x^2, \ldots, x^{d-1}, x^d = 1$ удовлетворяют уравнению $x^d = 1$, и это все корни данного уравнения. Сколько из этих d элементов имеют порядок, равный *в точности* d? Ответ очевиден: число таких элементов равно количеству целых чисел из $\{1, 2, \ldots, d-1, d\}$, взаимно простых с d (т. е. не имеющих общих делителей с d, кроме 1). Это количество обозначается $\varphi(d)$. Итак, порядок d имеют не более чем $\varphi(d)$ элементов из $\mathbb{F}_q^\times$. Утверждается, что для любого d — делителя $q-1$ число элементов из $\mathbb{F}_q^\times$, имеющих порядок d, равно $\varphi(d)$. Этот факт будет выведен из следующей леммы.

Лемма. $\sum_{d \mid n} \varphi(d) = n$.

Доказательство леммы. Пусть $\mathbb{Z}/n\mathbb{Z}$ обозначает аддитивную группу $\{0, 1, \ldots, n-1\}$ целых чисел по модулю n. Каждому делителю d числа n соответствует ее подгруппа S_d, состоящая из элементов $\mathbb{Z}/n\mathbb{Z}$, кратных n/d. Очевидно, любая подгруппа в $\mathbb{Z}/n\mathbb{Z}$ получается таким способом.

Подгруппа S_d состоит из d элементов, $\varphi(d)$ из которых порождают ее (потому что множество элементов, кратных mn/d в $\mathbb{Z}/n\mathbb{Z}$, совпадает с множеством элементов, кратных n/d, тогда и только тогда, когда m и d взаимно просты). С другой стороны, каждое из чисел $0, 1, \ldots, n-1$ порождает одну из таких под-

групп S_d. Следовательно,

$$\{0, 1, \ldots, n-1\} = \bigcup_{d \mid n} \{\text{элементы, порождающие } S_d\}.$$

Множества этого объединения не пересекаются, поэтому $n = \sum_{d \mid n} \varphi(d)$. Лемма доказана.

Из нее немедленно вытекает предложение, ибо если число элементов порядка d для некоторого $d \mid n\,(=q-1)$ меньше $\varphi(d)$, то $n = \sum_{d \mid n}$ (число элементов порядка $d) < \sum_{d \mid n} \varphi(d) = n$. Следовательно, в частности, существует $\varphi(q-1)$ элементов порядка $q-1$. Так как $\varphi(q-1) \geqslant 1$ (например, 1 взаимно проста с $q-1$), то найдется элемент a порядка точно $q-1$. Тогда $\mathbb{F}_q^\times = \{a, a^2, \ldots, a^{q-1}\}$. □

Упражнения

1. Пусть F — поле, состоящее из $q = p^f$ элементов. Докажите, что F содержит (единственное) подполе из $q' = p^{f'}$ элементов тогда и только тогда, когда f' делит f.

2. Для $p = 2, 3, 5, 7, 11$ и 13 найдите некоторый элемент $a \in \{1, 2, \ldots, p-1\}$, порождающий $\mathbb{F}_p^\times$, т. е. такой, что $\mathbb{F}_p^\times = \{a, a^2, \ldots, a^{p-1}\}$. В каждом из этих случаев определите число всевозможных выборов таких a.

3. Пусть F — множество выражений вида $a+bj$, где $a, b \in \mathbb{F}_3 = \{0, 1, 2\}$. На этом множестве определим сложение покомпонентно, а умножение — по формуле $(a+bj)(c+dj) = (ac+2bd) + (ad+bc)j$. Покажите, что $F = \mathbb{F}_9$, а $1+j$ — образующая в $\mathbb{F}_9^\times$. Найдите все образующие для $\mathbb{F}_9^\times$.

4. Опишите явно $\mathbb{F}_4$ и $\mathbb{F}_8$ способом, аналогичным использованному в предыдущем упражнении для $\mathbb{F}_9$. Объясните, почему любой элемент из $\mathbb{F}_4^\times$ или $\mathbb{F}_8^\times$ является образующей.

5. Пусть $q = pf$, а α — элемент, порождающий $\mathbb{F}_q^\times$. Обозначим через $P(X)$ минимальный многочлен элемента α над $\mathbb{F}_p$. Докажите, что $\deg P = f$.

6. Пусть $q=p^f$. Докажите, что все f автоморфизмов поля $\mathbb{F}_q$ над $\mathbb{F}_p$ исчерпываются автоморфизмами σ_i, $i=0, 1, \ldots, f-1$, следующего вида: $\sigma_i(x)=x^{p^i}$ для $x\in\mathbb{F}_q$.

7. Пусть $\alpha\in\mathbb{F}_p^\times$, а $P(X)=X^p-X-\alpha$. Покажите, что если a — корень многочлена $P(X)$, то элементы $a+1$, $a+2$ и т. д. также являются его корнями. Кроме того, покажите, что поле, полученное присоединением a к $\mathbb{F}_p$, имеет степень p над $\mathbb{F}_p$, т. е. изоморфно $\mathbb{F}_{p^p}$.

8. Докажите, что $\mathbb{F}_q$ содержит квадратный корень из -1 тогда и только тогда, когда $q\not\equiv 3 \pmod 4$.

9. Пусть ξ — некоторое алгебраическое число степени n над $\mathbb{Q}_p$, т. е. ξ является корнем многочлена степени n с коэффициентами в $\mathbb{Q}_p$ и не является корнем никакого такого многочлена меньшей степени. Докажите существование целого числа N, для которого ξ не удовлетворяет ни одному из сравнений вида

$$a_{n-1}\xi^{n-1}+a_{n-2}\xi^{n-2}+\ldots+a_1\xi+a_0\equiv 0 \pmod{p^N},$$

где a_i — целые рациональные числа, не все из которых делятся на p. (*Указание.* Предположите противное, а затем воспользуйтесь тем же подходом, что и в упр. 18 к § I.2 или в упр. 18 к § I.5.)

10. Пусть F — *произвольное* поле, а $f(X)=X^n+a_{n-1}X^{n-1}+\ldots+a_1X+a_0$ — многочлен с коэффициентами в F, распадающийся на линейные множители над F, т. е. $f(X)=\prod_{i=1}^{n}(X-\alpha_i)$, где $\alpha_i\in F$. Покажите, что всякий кратный корень α_i этого многочлена является также корнем для $nX^{n-1}+a_{n-1}(n-1)X^{n-2}+a_{n-2}\times\times(n-2)X^{n-3}+\ldots+a_1$.

§ 2. ПРОДОЛЖЕНИЕ НОРМ

Метрическое пространство X называется (секвенциально) *компактным*, если каждая последовательность его элементов имеет сходящуюся подпоследовательность (см. начало § II.3). Например, $\mathbb{Z}_p$ — компактное метрическое пространство (см. упр. 18 к § I.5). Пространство X называется *локально компактным*, если каждая точка $x\in X$ обладает некоторой компактной окрестностью (т. е. компактным подмножеством в X, содержащим диск $\{y\mid d(x, y)<\varepsilon\}$ для некоторого $\varepsilon>0$). Множество вещественных чисел $\mathbb{R}$ с обычной архимедовой метрикой, индуцированной абсолютной величиной, локально компактно, но не компактно. Другой пример

локально компактного метрического пространства дает поле $\mathbb{Q}_p$ с p-адической метрикой. В самом деле, для любой точки x окрестность $x+\mathbb{Z}_p \overset{\text{def}}{=} \{y \mid |y-x|_p \leqslant 1\}$ компактна (ибо она изоморфна $\mathbb{Z}_p$ как метрическое пространство). Эти примеры можно включить в следующую более общую картину. Пусть X — метрическое пространство, обладающее структурой аддитивной группы, такой, что $d(x, y) = d(x-y, 0)$ для любых x, y (например, X — векторное пространство с метрикой, индуцированной нормой на X; определение см. ниже). Тогда X локально компактно всякий раз, когда 0 имеет компактную окрестность U. Действительно, для любой точки x окрестность $x+U \overset{\text{def}}{=} \{y \mid y-x \in U\}$ (сдвиг U на x) компактна. Для $\mathbb{Q}_p$ в качестве компактной окрестности 0 можно взять $U=\mathbb{Z}_p$. Нетрудно установить (см. ниже упр. 6) полноту каждой такой локально компактной группы.

Пусть F — некоторое поле с неархимедовой нормой $\| \|$. До конца данного параграфа будем предполагать F локально компактным.

Пусть V — конечномерное векторное пространство над F. Норму на векторном пространстве V можно определить по аналогии с нормой в поле. А именно, отображение $\| \|_V$ из V в множество неотрицательных вещественных чисел называется *нормой* на V, если: (1) $\|x\|_V = 0$ тогда и только тогда, когда $x=0$; (2) $\|ax\|_V = \|a\| \|x\|_V$ для всех $x \in V$ и $a \in F$ (где $\|a\|$ есть норма в F); (3) $\|x+y\|_V \leqslant \|x\|_V + \|y\|_V$. Например, если K — конечное расширение поля F, то всякая норма на поле K, ограничение которой совпадает с $\| \|$ на F, есть норма на K, рассматриваемом как векторное пространство над F. Сразу же предупредим, что обратное, вообще говоря, не верно, так как свойство (2) нормы векторного пространства слабее соответствующего свойства нормы поля (см. ниже упр. 3 — 4).

Как и в случае полей, две нормы $\| \|_1$ и $\| \|_2$ на V считаются эквивалентными, если отвечающие им множества последовательностей Коши совпадают. Это свойство выполнено в том и только том случае, когда существуют две положительные константы c_1 и c_2, для

которых $\|x\|_2 \leqslant c_1 \|x\|_1$ и $\|x\|_1 \leqslant c_2 \|x\|_2$ при любых $x \in V$ (см ниже упр. 1).

Теорема 10. *Пусть V — конечномерное векторное пространство над локально компактным полем F. Тогда все нормы на V эквивалентны.*

Доказательство. Пусть $\{v_1, \ldots, v_n\}$ — некоторый базис в V. Определим на V функцию $\| \|_{\sup}$ формулой

$$\|a_1 v_1 + \ldots + a_n v_n\|_{\sup} \overset{\text{def}}{=} \max_{1 \leqslant i \leqslant n} (\|a_i\|).$$

Эта функция $\| \|_{\sup}$ является нормой (см. ниже упр. 2). Мы будем называть ее sup-нормой. Пусть теперь $\| \|_V$ — некоторая другая норма на V. Прежде всего для любого $x = a_1 v_1 + \ldots + a_n v_n$ выполнены неравенства

$$\|x\|_V \leqslant \|a_1\| \|v_1\|_V + \ldots + \|a_n\| \|v_n\|_V \leqslant$$
$$\leqslant n (\max \|a_i\|) \max \|v_i\|_V.$$

Поэтому $\| \|_V \leqslant c_1 \| \|_{\sup}$, где $c_1 = n \max\limits_{1 \leqslant i \leqslant n} (\|v_i\|_V)$. Таким образом, если мы найдем константу c_2, для которой будет выполнено братное неравенство, то тем самым установим эквивалентность любой нормы на V sup-норме. Пусть

$$U = \{x \in V \mid \|x\|_{\sup} = 1\}.$$

Тогда утверждается, что существует положительное ε, для которого $\|x\|_V \geqslant \varepsilon$ при любом $x \in U$. Предположим противное. В этом случае можно найти такую последовательность $\{x_i\}$ элементов U, что $\|x_i\|_V \to 0$. В силу компактности U относительно $\| \|_{\sup}$ (см. ниже упр. 2, 8) существует подпоследовательность $\{x_{i_j}\}$, сходящаяся относительно sup-нормы к некоторому $x \in U$. Но по доказанному выше неравенству

$$\|x\|_V \leqslant \|x - x_{i_j}\|_V + \|x_{i_j}\|_V \leqslant c_1 \|x - x_{i_j}\|_{\sup} + \|x_{i_j}\|_V$$

для любого j. Оба последних члена стремятся к 0 при $j \to \infty$, так как x_{i_j} стремится к x относительно $\| \|_{\sup}$, а $\|x_i\|_V \to 0$. Следовательно, $\|x\|_V = 0$, откуда $x = 0 \notin U$ — противоречие.

Используя это утверждение, теперь нетрудно доказать второе неравенство, а с ним и теорему. Идея рассуждения такова. Как было установлено, норма $\| \|_V$ на единичной сфере U относительно $\| \|_{\sup}$ принимает значения $\geqslant \varepsilon > 0$. Следовательно, $\| \|_{\sup} \leqslant c_2 \| \|_V$ на U, где $c_2 = 1/\varepsilon$ (левая часть по определению равна 1 на U). С другой стороны, все векторы из V можно получить, умножая векторы, лежащие в U, на элементы поля F. Поэтому такое же неравенство справедливо на всем V.

Точнее, пусть $x = a_1 v_1 + \ldots + a_n v_n$ — произвольный ненулевой элемент из V. Выберем такое j, что $\|a_j\| = \max \|a_i\| = \|x\|_{\sup}$. Тогда, очевидно, $(x/a_j) \in U$ и $\|x/a_j\|_V \geqslant \varepsilon = 1/c_2$. Поэтому

$$\|x\|_{\sup} = \|a_j\| \leqslant c_2 \|x\|_V. \quad \square$$

Следствие. *Пусть $V = K$ — некоторое поле. Тогда существует не более одного продолжения нормы $\| \|$, заданной на F, до нормы $\| \|_K$ на K (т. е. такой, что $\|a\|_K = \|a\|$ для $a \in F$).*

Доказательство следствия. Любые две такие нормы $\| \|_1$ и $\| \|_2$ эквивалентны по теореме 10. Следовательно, $\| \|_2 \leqslant c_1 \| \|_1$. Рассмотрим $x \in K$, для которого $\|x\|_1 \neq \|x\|_2$, скажем $\|x\|_1 < \|x\|_2$. Тогда при достаточно большом N получается противоречие: $c_1 \|x^N\|_1 < \|x^N\|_2$. $\square$

Это следствие, однако, оставляет открытым вопрос о существовании хотя бы одного продолжения $\| \|$ с F на K.

Напомним теперь одно из основных понятий, относящихся к расширениям полей: понятие «нормы» элемента. Новое словоупотребление не следует путать с прежним, относившимся к метрическим пространствам. «Норма» в новом смысле будет всегда в кавычках, и для нее мы введем специальное обозначение $\mathbb{N}$.

Пусть $K = F(\alpha)$ — конечное расширение поля F, порожденное некоторым элементом α с минимальным многочленом

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n, \quad a_i \in F,$$

Тогда «норма элемента α из K в F», обозначаемая через $N_{K/F}(\alpha)$, определяется одним из трех эквивалентных способов.

(1) Если K рассматривать как векторное пространство над F, то умножение на α задает F-линейное отображение с матрицей A_α в некотором базисе. Полагаем $N_{K/F}(\alpha) \overset{\text{def}}{=} \det(A_\alpha)$.

(2) $N_{K/F}(\alpha) \overset{\text{def}}{=} (-1)^n a_n$.

(3) $N_{K/F}(\alpha) \overset{\text{def}}{=} \prod_{i=1}^{n} \alpha_i$, где через α_i обозначены все элементы, сопряженные с $\alpha = \alpha_1$ над F.

Эквивалентность (2) $\Leftrightarrow$ (3) следует из соотношения $x^n + a_1 x^{n-1} + \ldots + a_n = \prod_{i=1}^{n} (x - \alpha_i)$. Для доказательства эквивалентности (1) $\Leftrightarrow$ (2) возьмем в K над F базис $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Тогда матрица оператора умножения на α примет вид

$$\begin{pmatrix} 0 & 0 & & & -a_n \\ 1 & 0 & 0 & & -a_{n-1} \\ & 1 & 0 & & \vdots \\ & & & \ddots & \vdots \\ & & & 0 & -a_2 \\ & & & 1 & -a_1 \end{pmatrix}$$

(поскольку $\alpha^n = -a_1\alpha^{n-1} - \ldots - a_{n-1}\alpha - a_n$). Из разложения определителя этой матрицы по первой строке видно, что он равен $(-1)^n a_n$.

Пусть $\beta \in K = F(\alpha)$. Тогда $N_{K/F}(\beta)$ определяется одним из двух способов: (1) как определитель матрицы линейного оператора умножения на β в K или (эквивалентно) (2) как $(N_{F(\beta)/F}(\beta))^{[K:F(\beta)]}$. Для доказательства эквивалентности выберем базис в $F(\beta)$ как векторном пространстве над F, а также в K как векторном пространстве над $F(\beta)$. Тогда в качестве базиса K над F можно взять все попарные произведения элементов первого и второго базисов. В этом базисе

(при подходящем порядке элементов) матрица умножения на β «распадается на блоки»

$$\begin{pmatrix} A_\beta & 0 & & \\ 0 & A_\beta & & \\ & & \ddots & \\ & & & A_\beta \end{pmatrix},$$

где A_β — матрица умножения на β в $F(\beta)$. Определитель этой матрицы равен $[K : F(\beta)]$-й степени ($[K : F(\beta)]$ — это число блоков) $\det A_\beta$, т. е. $[K : F(\beta)]$-й степени элемента $N_{F(\beta)/F}(\beta)$. Итак, два определения действительно эквивалентны.

Из первого определения $N_{K/F}(\alpha)$ для *любого* $\alpha \in K$ как определителя оператора умножения на α в K следует *мультипликативность* отображения $N_{K/F}$ из K в F, т. е. $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha) N_{K/F}(\beta)$. (В самом деле, матрица умножения на $\alpha\beta$ равна произведению матриц умножения на α и на β, а определитель произведения матриц равен произведению определителей сомножителей.)

Теперь можно догадаться, каким должно быть выражение для продолженной нормы $|\ |_p$ алгебраического числа $\alpha \in \mathbb{Q}_p^{\text{alg cl}}$, если такая норма существует. Предположим, что α имеет степень n, т. е. минимальный многочлен этого элемента над $\mathbb{Q}_p$ имеет степень n. Пусть K — конечное *расширение Галуа* поля $\mathbb{Q}_p$, содержащее α (см. пункт (10) в § 1). В качестве K можно взять, например, поле, полученное присоединением α и всех его сопряженных к $\mathbb{Q}_p$ (как легко проверить, это конечное расширение Галуа над $\mathbb{Q}_p$). Предположим, что найдено некоторое продолжение $\|\ \|$ нормы $|\ |_p$ на K. Эта норма $\|\ \|$ на K *единственна* в силу следствия из теоремы 10. Пусть теперь α' — элемент, сопряженный с α, а σ — некоторый автоморфизм поля K, переводящий α в α' (см. пункты (8), (9) и (11) в § 1). Очевидно, отображение $\|\ \|' : K \to \mathbb{R}$, заданное соотношением $\|x\|' = \|\sigma(x)\|$, является также продолжением нормы $|\ |_p$ на K. Следовательно, $\|\ \|' = \|\ \|$, откуда $\|\alpha\| = \|\alpha\|' = \|\sigma(\alpha)\| = \|\alpha'\|$. Значит, *норма элемента* α *равна норме каждого сопряженного с ним элемента*. С другой стороны, норма

элемента $N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)$, лежащего в $\mathbb{Q}_p$, равна

$$|N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p = \|N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)\| = \left\| \prod_{\text{сопряженные } \alpha' \text{ с } \alpha} \alpha' \right\| = \prod \|\alpha'\| = \|\alpha\|^n.$$

Поэтому

$$\|\alpha\| = |N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p^{1/n}.$$

Итак, для того чтобы найти p-адическую норму числа α, следует посмотреть на его минимальный многочлен. Если он имеет степень n и постоянный член a_n, то p-адическая норма α равна корню степени n из $|a_n|_p$. (Конечно, мы еще не доказали, что это правило определяет функцию, обладающую всеми необходимыми свойствами нормы; это будет доказано ниже в теореме 11.)

Отметим следующее эквивалентное определение $\|\alpha\|$:

$$|N_{K/\mathbb{Q}_p}(\alpha)|_p^{1/[K:\mathbb{Q}_p]},$$

где K — произвольное конечное расширение, содержащее α. Действительно,

$$N_{K/\mathbb{Q}_p}(\alpha) = (N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p})^{[K:\mathbb{Q}_p(\alpha)]}$$

и $$n = [\mathbb{Q}_p(\alpha):\mathbb{Q}_p] = \frac{[K:\mathbb{Q}_p]}{[K:\mathbb{Q}_p(\alpha)]}.$$

Докажем теперь, что указанное правило вычисления $\|\ \|$ действительно задает норму. Ниже мы будем писать $|\ |_p$ вместо $\|\ \|$, указывая тем самым, что $\|\ \|$ продолжает $|\ |_p$. Это не должно приводить к путанице. Следует предупредить читателя, что теорему 11 доказать нелегко. Доказательство, изложенное ниже, которое я узнал от Д. Каждана, гораздо эффективнее других известных мне доказательств. Однако и его следует внимательно прочесть и перечесть, пока читатель не продумает рассуждения со всей основательностью.

Теорема 11. *Пусть K — конечное расширение поля $\mathbb{Q}_p$. Тогда на K существует некоторая норма, продолжающая норму $|\ |_p$ с $\mathbb{Q}_p$.*

Доказательство. Пусть $n=[K:\mathbb{Q}_p]$. Сначала мы определим $|\ |_p$ на K, а затем докажем, что эта функция в самом деле является нормой на K, продолжающей норму $|\ |_p$ с $\mathbb{Q}_p$. Для произвольного $\alpha\in K$ положим

$$|\alpha|_p \underset{\text{def}}{=} |N_{K/\mathbb{Q}_p}(\alpha)|_p^{1/n},$$

где справа стоит определенная ранее норма на $\mathbb{Q}_p$. Легко проверить, что: (1) новое значение $|\alpha|_p$ совпадает с определенным ранее $|\alpha|_p$ для всех $\alpha\in\mathbb{Q}_p$; (2) $|\alpha|_p$ мультипликативна и (3) $|\alpha|_p=0\Leftrightarrow\alpha=0$. Трудная часть — доказательство свойства $|\alpha+\beta|_p\leqslant$ $\leqslant\max(|\alpha|_p,\ |\beta|_p)$.

Предположим, что $|\beta|_p=\max(|\alpha|_p,\ |\beta|_p)$. Тогда, положив $\gamma=\alpha/\beta$, мы видим, что достаточно доказать неравенство

$$|1+\gamma|_p\leqslant 1 \quad \text{для всех } \gamma \text{ с } |\gamma|_p\leqslant 1.$$

Допустим сначала, что γ — «примитивный элемент» поля, т. е. $K=\mathbb{Q}_p(\gamma)$. Возьмем в качестве базиса векторного пространства K над $\mathbb{Q}_p$ набор $\{1,\gamma,\gamma^2,\ldots,\gamma^{n-1}\}$. Пусть A — матрица умножения на γ. Тогда A^i — матрица умножения на γ^i. Кроме того, $|\gamma|_p=|\det A|_p^{1/n}$, а $|1+\gamma|_p=|\det(1+A)|_p^{1/n}$. Пусть $\|\ \|$ обозначает sup-норму на n^2-мерном $\mathbb{Q}_p$-векторном пространстве $n\times n$-матриц с элементами в $\mathbb{Q}_p$. Утверждается, что последовательность значений $\{\|A^i\|\}$ ограничена.

Предположим противное. Тогда существует такая последовательность индексов i_j, что $\|A^{i_j}\|=b_j>j$. Пусть β_j — «максимальный» элемент матрицы A^{i_j}, т. е. $|\beta_j|_p=$ $=\max|\beta|_p=\|A^{i_j}\|$, где максимум берется по всем элементам β матрицы A^{i_j}. Рассмотрим последовательность матриц

$$B_j \underset{\text{def}}{=} A^{i_j}/\beta_j.$$

Очевидно, $\|B_j\|=1$. Единичная сфера в sup-норме компактна (см. ниже упр. 2 и 8), поэтому можно найти подпоследовательность $\{B_{j_k}\}$, сходящуюся в этой норме

к некоторой матрице B. Так как $\det B_j = \det A^{ij}/\beta_j^n$, то

$$|\det B_j|_p < |\det A^{ij}|_p / j^n = |\gamma|_p^{nij}/j^n \leqslant 1/j^n.$$

Но $B_{j_k} \to B$, т. е. максимум $|\ |_p$ от элементов матрицы $B_{j_k} - B$ стремится к 0, поэтому $\det B_{j_k}$ стремится к $\det B$. Следовательно, $\det B = 0$.

Таким образом, существует ненулевой элемент $l \in K$, для которого $B(l) = 0$. Покажем, что из этого следует тождественное обращение в нуль матрицы B, что противоречит равенству $\|B\| = 1$.

Достаточно установить соотношение $B(\gamma^i l) = 0$ для любого i, так как $\{\gamma^i l\}_{i=0}^{n-1}$ — базис в K. Но

$$B(\gamma^i l) = \lim_{k\to\infty} B_{j_k}(\gamma^i l) = \lim_{k\to\infty} \gamma^i B_{j_k}(l)$$

(потому что B_{j_k} — матрица умножения на степень γ, деленная на элемент β_{j_k} из $\mathbb{Q}_p$). Последний предел равен

$$\gamma^i \lim_{k\to\infty} B_{j_k}(l) = \gamma^i B(l) = 0.$$

Следовательно, $\{\|A^i\|\}$ ограничена некоторой константой C.

Отметим, что для любой $n\times n$-матрицы $A = \{a_{ij}\}$ выполнено неравенство $|\det A|_p \leqslant (\max\limits_{i,\ j} |a_{ij}|_p)^n = \|A\|^n$. В этом легко убедиться, если разложить определитель и воспользоваться аддитивными и мультипликативными свойствами неархимедовой нормы.

Теперь возьмем достаточно большое N и рассмотрим разложение

$$(1+A)^N = 1 + \binom{N}{1} A + \ldots + \binom{N}{N-1} A^{N-1} + A^N.$$

Тогда

$$|1+\gamma|_p^N = |\det (1+A)^N|_p^{1/n} \leqslant \|(1+A)^N\| \leqslant$$
$$\leqslant \max_{0\leqslant l\leqslant N} \left\|\binom{N}{l} A^l\right\| \leqslant \max_{0\leqslant i\leqslant N} \|A^i\| \leqslant C.$$

Следовательно, $|1+\gamma|_p \leqslant \sqrt[N]{C}$. Переходя к пределу при $N\to\infty$, мы получаем требуемое неравенство $|1+\gamma|_p \leqslant 1$.

(Отметим сходство этого доказательства с доказательством теоремы Островского в § I.2.)

Если γ — не примитивный элемент, то, заменяя K на $\mathbb{Q}_p(\gamma)$, мы получим $1 \geqslant |N_{\mathbb{Q}_p(\gamma)/\mathbb{Q}_p}(1+\gamma)|_p^{1/[\mathbb{Q}_p(\gamma):\mathbb{Q}_p]} = |N_{K/\mathbb{Q}_p}(1+\gamma)|_p^{1/n} = |1+\gamma|_p$. Это неравенство завершает доказательство теоремы 11. □

Пусть R — (коммутативное) *кольцо*, т. е. множество с двумя операциями $+$ и $\cdot$, удовлетворяющими всем требованиям, предъявляемым к полю[1]), кроме, возможно, существования мультипликативно обратных элементов. Иначе говоря, это аддитивная группа относительно $+$; выполнены ассоциативность, коммутативность и существует единица относительно $\cdot$; кроме того, имеет место дистрибутивность. Кольцо R называется *областью целостности*, если из $xy=0$ всегда следует, что $x=0$ или $y=0$. Примеры областей целостности — кольца $\mathbb{Z}$ и $\mathbb{Z}_p$.

Собственное подмножество I кольца R называется *идеалом*, если оно является подгруппой в R относительно сложения и для всех $x \in R$ и $a \in I$ справедливо включение $xa \in I$. В кольце $\mathbb{Z}$ множество всех чисел, кратных некоторому фиксированному целому числу, задает идеал. В $\mathbb{Z}_p$ для любого $r \leqslant 1$ множество $\{x \in \mathbb{Z}_p \mid |x|_p < r\}$ есть идеал. Если, например, $r = p^{-n}$, то это множество всех целых p-адических чисел, первые $n+1$ знаков которых в p-адическом разложении равны нулю.

Пусть I_1 и I_2 — два идеала из R. Тогда легко проверить, что множество

$$\{x \in R \mid x \text{ представимо в виде } x = x_1x_1' + \ldots + x_mx_m' \text{ с } x_i \in I_1 \text{ и } x_i' \in I_2\}$$

также является идеалом. Этот идеал обозначается через I_1I_2 и называется произведением двух данных идеалов. Идеал I называется *простым*, если из включения $x_1x_2 \in I$ следует, что $x_1 \in I$ или $x_2 \in I$[2]).

---

[1]) В частности, $1 \neq 0$. — *Прим. перев.*

[2]) Заметим, что в этой книге все идеалы предполагаются собственными. — *Прим. перев.*

Легко проверить, что кольцо $\mathbb{Z}_p$ имеет единственный простой идеал ($\neq\{0\}$) (см. ниже упр. 5), а именно:

$$p\mathbb{Z}_p \underset{\text{def}}{=} \{x \in \mathbb{Z}_p \mid |x|_p < 1\}.$$

Кроме того, все идеалы ($\neq\{0\}$) кольца $\mathbb{Z}_p$ имеют вид

$$p^n\mathbb{Z}_p \underset{\text{def}}{=} \{x \in \mathbb{Z}_p \mid |x|_p \leqslant p^{-n}\}.$$

Пусть I — некоторый идеал кольца R. Тогда легко установить, что аддитивные классы смежности $x+I$ образуют кольцо. Это кольцо обозначается R/I и называется факторкольцом кольца R по идеалу I. (Другой способ описать это кольцо заключается в рассмотрении классов эквивалентности элементов из R по такому отношению: $x \sim y$, если $x-y \in I$.) Например, если $R=\mathbb{Z}$ (или $R=\mathbb{Z}_p$), то, как было установлено выше, кольцо R/pR совпадает с полем $\mathbb{F}_p$ из p элементов.

Идеал M из R называется *максимальным*, если не существует такого идеала I, что $M \subset I \subset R$ (оба включения строгие). Оставим в качестве легкого упражнения проверку следующих фактов.

(1) Идеал P прост тогда и только тогда, когда R/P — область целостности.

(2) Идеал M максимален тогда и только тогда, когда R/M — поле.

Предположим теперь, что K — некоторое конечное расширение поля $\mathbb{Q}_p$. (Или, более общо, пусть K — алгебраическое расширение поля частных F некоторой области целостности R, например: $F=\mathbb{Q}$ — поле частных для $R=\mathbb{Z}$, $F=\mathbb{Q}_p$ — поле частных для $R=\mathbb{Z}_p$ и т. д.) Пусть A — множество всех элементов $x \in K$, удовлетворяющих уравнению вида $x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n=0$ с $a_i \in \mathbb{Z}_p$. (Конечно, каждый $x \in K$ удовлетворяет такому уравнению с коэффициентами a_i из $\mathbb{Q}_p$, но они не обязаны лежать в $\mathbb{Z}_p$.) Множество A называется *целым замыканием кольца* $\mathbb{Z}_p$ *в* K.

Нетрудно показать, что минимальный многочлен любого элемента $x \in A$ имеет указанный вид. Кроме того, целое замыкание всегда является кольцом. (Общее доказательство см. у Ленга [(a) 3], стр. 268 — 275.

Случай, который нам необходим в дальнейшем, — целое замыкание $\mathbb{Z}_p$ в K — рассмотрен в следующем предложении.)

Предложение. *Пусть K — конечное расширение степени n поля $\mathbb{Q}_p$ и*

$$A=\{x\in K \mid |x|_p\leqslant 1\},\quad M=\{x\in K \mid |x|_p<1\}.$$

Тогда A — кольцо, совпадающее с целым замыканием кольца $\mathbb{Z}_p$ в K, M — единственный максимальный идеал этого кольца, а A/M — конечное расширение поля $\mathbb{F}_p$ степени, не превосходящей n.

Доказательство. Используя мультипликативное и аддитивное свойства неархимедовой нормы, легко проверить, что A — кольцо, а M — его идеал. Пусть теперь $\alpha\in K$ — некоторый элемент степени m над $\mathbb{Q}_p$. Предположим, что α цел над $\mathbb{Z}_p$: $\alpha^m+a_1\alpha^{m-1}+\ldots+a_m=0$, $a_i\in\mathbb{Z}_p$. Предположив, что $|\alpha|_p>1$, мы придем к противоречию:

$$|\alpha|_p^m=|\alpha^m|_p=|a_1\alpha^{m-1}+\ldots+a_m|_p\leqslant \max_{1\leqslant i\leqslant m}|a_i\alpha^{m-i}|_p\leqslant$$

$$\leqslant \max_{1\leqslant i\leqslant m}|\alpha^{m-i}|_p=|\alpha|_p^{m-1}.$$

Обратно, пусть $|\alpha|_p\leqslant 1$. Тогда для всех сопряженных с $\alpha=\alpha_1$ над $\mathbb{Q}_p$ также $|\alpha_i|_p=\prod_{j=1}^{m}|\alpha_j|_p^{1/m}=|\alpha|_p\leqslant 1$. Так как все коэффициенты минимального многочлена для α равны суммам произведений α_i (*симметрическим многочленам* от α_i), для этих коэффициентов также $|\ |_p\leqslant 1$. Следовательно, они должны лежать в $\mathbb{Z}_p$, поскольку они лежат в $\mathbb{Q}_p$.

Докажем теперь, что M содержит каждый идеал из A. Предположим, что $\alpha\in A$ и $\alpha\notin M$. Тогда $|\alpha|_p=1$, откуда $|1/\alpha|_p=1$ и $1/\alpha\in A$. Поэтому любой идеал, содержащий α, должен содержать $(1/\alpha)\cdot\alpha=1$, что невозможно.

Отметим, что $M\cap\mathbb{Z}_p=p\mathbb{Z}_p$ по определению M.

Рассмотрим поле A/M. Напомним, что элементы этого поля суть классы смежности $a+M$. Заметим, что

если a и b окажутся в $\mathbb{Z}_p$, то класс $a+M$ совпадет с $b+M$ в том и только том случае, когда $a-b \in M \cap \mathbb{Z}_p = p\mathbb{Z}_p$. Отсюда получается естественное вложение $\mathbb{Z}_p/p\mathbb{Z}_p$ в A/M, задаваемое отображением (класс $a+p\mathbb{Z}_p) \longmapsto$ (класс $a+M$) для $a \in \mathbb{Z}_p$. Так как $\mathbb{Z}_p/p\mathbb{Z}_p$ есть поле $\mathbb{F}_p$, состоящее из p элементов, то A/M — расширение этого поля $\mathbb{F}_p$.

Утверждается, что A/M имеет конечную степень над $\mathbb{F}_p$. Точнее, установим неравенство $[A/M:\mathbb{F}_p] \leqslant [K:\mathbb{Q}_p]$. Для этого покажем, что любая система из $n+1$ элементов $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_{n+1} \in A/M$ линейно зависима над $\mathbb{F}_p$, где $n=[K:\mathbb{Q}_p]$. Для $i=1, 2, \ldots, n+1$ выберем элемент a_i в A, который переходит в класс $\bar{a}_i$ при отображении $A \to A/M$ (т. е. a_i — некоторый элемент класса смежности $\bar{a}_i$, или, другими словами, $\bar{a}_i = a_i + M$). Так как $[K:\mathbb{Q}_p]=n$, то $a_1, a_2, \ldots, a_{n+1}$ линейно зависимы над $\mathbb{Q}_p$:

$$a_1b_1 + a_2b_2 + \ldots + a_{n+1}b_{n+1} = 0, \quad b_i \in \mathbb{Q}_p.$$

После умножения на подходящую степень p можно предполагать, что все $b_i \in \mathbb{Z}_p$ и по крайней мере одно b_i не лежит в $p\mathbb{Z}_p$. После факторизации это выражение превращается в равенство

$$\bar{a}_1\bar{b}_1 + \bar{a}_2\bar{b}_2 + \ldots + \bar{a}_{n+1}\bar{b}_{n+1} = 0$$

в A/M, где $\bar{b}_i$ — образ b_i в $\mathbb{Z}_p/p\mathbb{Z}_p$ (т. е. $\bar{b}_i$ определяется первым знаком p-адического разложения b_i). Поскольку по крайней мере одно b_i не принадлежит $p\mathbb{Z}_p$, то одно из $\bar{b}_i$ не равно 0. Поэтому, как и утверждалось, $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_{n+1}$ линейно зависимы. □

Поле A/M называется *полем вычетов* для K. Это расширение поля $\mathbb{F}_p$ некоторой конечной степени f. Кольцо A называется *кольцом нормирования*, соответствующим $|\ |_p$, в K.

Упражнения

1. Докажите, что две нормы $\|\ \|_1$ и $\|\ \|_2$ на конечномерном векторном пространстве эквивалентны в том и только том случае, когда существуют такие константы $c_1 > 0$ и $c_2 > 0$, что при всех $x \in V$

$$\|x\|_2 \leqslant c_1 \|x\|_1 \quad \text{и} \quad \|x\|_1 \leqslant c_2 \|x\|_2.$$

2. Пусть F — поле с нормой $\| \|$, а V — конечномерное векторное пространство над F с базисом $\{v_1, \ldots, v_n\}$. Покажите, что функция $\|a_1v_1+\ldots+a_nv_n\|_{\sup} \underset{\text{def}}{=} \max_{1\leqslant i\leqslant n} (\|a_i\|)$ является нормой на V. Докажите, что из локальной компактности F следует локальная компактность V.

3. Пусть $V=\mathbb{Q}_p(\sqrt{p})$, $v_1=1$, $v_2=\sqrt{p}$. Докажите, что sup-норма не будет нормой на *поле* $\mathbb{Q}_p(\sqrt{p})$.

4. Пусть $V=K$ — некоторое поле. Может ли вообще sup-норма быть нормой на этом поле (хоть для какого-нибудь базиса $\{v_1, \ldots, v_n\}$) при $n=\dim K>1$? Для каких конечных расширений K поля $\mathbb{Q}_p$ sup-норма никогда не является нормой на этом поле?

5. Докажите, что $\mathbb{Z}_p$ имеет единственный максимальный идеал $p\mathbb{Z}_p$ и что все идеалы ($\neq\{0\}$) из $\mathbb{Z}_p$ имеют вид $p^n\mathbb{Z}_p$, $n\in\{1, 2, 3, \ldots\}$.

6. Докажите, что всякое локально компактное векторное пространство V с нормой $\| \|_p$ полно.

7. Докажите, что векторное пространство с нормой $\| \|_V$ локально компактно тогда и только тогда, когда компактен шар $\{x \mid \|x\|_V\leqslant 1\}$.

8. Докажите компактность сферы $\{x \mid \|x\|_V=1\}$ для локально компактного векторного пространства с нормой $\| \|_V$.

§ 3. АЛГЕБРАИЧЕСКОЕ ЗАМЫКАНИЕ ПОЛЯ $\mathbb{Q}_p$

Сопоставляя две теоремы из § 2, мы видим, что $| |_p$ имеет единственное продолжение (которое также обозначается через $| |_p$) на любое конечное расширение поля $\mathbb{Q}_p$. Поскольку алгебраическое замыкание $\overline{\mathbb{Q}}_p$ поля $\mathbb{Q}_p$ является объединением таких расширений, норма $| |_p$ однозначно продолжается на $\overline{\mathbb{Q}}_p$. Точнее, если $\alpha\in\overline{\mathbb{Q}}_p$ имеет минимальный многочлен $x^n+a_1x^{n-1}+\ldots+a_n$, то $|\alpha|_p=|a_n|_p^{1/n}$.

Пусть K — расширение степени n поля $\mathbb{Q}_p$. Для $\alpha\in K$ положим

$$\operatorname{ord}_p\alpha \underset{\text{def}}{=} -\log_p|\alpha|_p=-\log_p|\mathrm{N}_{K/\mathbb{Q}_p}(\alpha)|_p^{1/n}=$$

$$=-\frac{1}{n}\log_p|\mathrm{N}_{K/\mathbb{Q}_p}(\alpha)|_p.$$

При $\alpha\in\mathbb{Q}_p$ значение $\operatorname{ord}_p\alpha$ совпадает с определенным ранее. Кроме того, очевидно свойство $\operatorname{ord}_p\alpha\beta=\operatorname{ord}_p\alpha+$

$+\operatorname{ord}_p\beta$. Образ K при отображении ord_p попадает в множество $(1/n)\mathbb{Z} \underset{\text{def}}{=} \{x \in \mathbb{Q} \mid nx \in \mathbb{Z}\}$. Этот образ есть аддитивная подгруппа в $(1/n)\mathbb{Z}$. Поэтому он представим в виде $(1/e)\mathbb{Z}$ для некоторого целого положительного e, делящего n. Это целое число e называется *индексом ветвления* поля K над $\mathbb{Q}_p$. Если $e=1$, то говорят, что K — *неразветвленное* расширение поля $\mathbb{Q}_p$. Пусть $\pi \in K$ — элемент, для которого $\operatorname{ord}_p\pi = 1/e$. Тогда, очевидно, любой $x \in K$ однозначно записывается в виде

$$\pi^m u, \quad \text{где } |u|_p = 1, \quad \text{а } m \in \mathbb{Z} \quad (\text{при этом } m = e\cdot\operatorname{ord}_p x).$$

Можно доказать (см. ниже упр. 12), что $n = e\cdot f$, где $n = [K:\mathbb{Q}_p]$, e — индекс ветвления, а f — степень расширения поля вычетов A/M над $\mathbb{F}_p$. Во всяком случае, мы уже знаем, что $f \leqslant n$ и $e \leqslant n$. Если K — неразветвленное расширение, т. е. $e=1$, то в качестве π из предыдущего абзаца можно взять p, потому что $\operatorname{ord}_p p = 1 = 1/e$. В другом крайнем случае, когда $e=n$, расширение K называется *вполне разветвленным*.

Предложение. *Пусть K — вполне разветвленное расширение, а $\pi \in K$ — такой элемент, что $\operatorname{ord}_p\pi = 1/e$. Тогда π удовлетворяет некоторому уравнению Эйзенштейна (см. упр. 13 к § 1.5)*

$$x^e + a_{e-1}x^{e-1} + \ldots + a_0 = 0,$$

где $a_i \equiv 0 \pmod p$ при всех i, а $a_0 \not\equiv 0 \pmod{p^2}$. Обратно, если α — корень некоторого такого уравнения Эйзенштейна над $\mathbb{Q}_p$, то $\mathbb{Q}_p(\alpha)$ — вполне разветвленное расширение степени e над $\mathbb{Q}_p$.

Доказательство. Прежде всего $|a_i|_p < 1$, так как a_i — значения симметрических полиномов от элементов, сопряженных с π и имеющих норму $|\ |_p = p^{-1/e}$. Что касается a_0, то $|a_0|_p = |\pi|_p^e = 1/p$.

Обратно, как видно из упр. 13 к § I.5, многочлен Эйзенштейна неприводим. Поэтому, присоединив его корень α, мы получим расширение степени e. Из равенства $\operatorname{ord}_p a_0 = 1$ следует, что $\operatorname{ord}_p\alpha = (1/e)\operatorname{ord}_p a_0 = 1/e$. Значит, $\mathbb{Q}_p(\alpha)$ вполне разветвлено над $\mathbb{Q}_p$. □

Более точное описание корней многочленов, присоединение которых задает вполне разветвленные расширения степени e, можно дать, если e не делится на p (в этом случае ветвление называется *ручным*; если $p \mid e$, ветвление называется *диким*). А именно, ручные вполне разветвленные расширения получаются присоединением решений уравнения $x^e - pu = 0$, где $u \in \mathbb{Z}_p^\times$, т. е. все такие расширения получаются добавлением корня степени e из произведения p на некоторую p-адическую единицу (см. ниже упр. 13 и 14).

Пусть теперь K — произвольное конечное расширение поля $\mathbb{Q}_p$. Следующее предложение утверждает, что если K не разветвлено, т. е. $e = 1$, то K имеет очень специальный вид: получается присоединением некоторого корня из 1. В случае же, когда K разветвлено, вначале следует построить его максимальное неразветвленное подполе, присоединяя некоторый подходящий корень из 1, а затем исходное расширение получается присоединением корня некоторого многочлена Эйзенштейна. *Предупреждение*: доказательство следующего предложения несколько утомительно, и читатель, который спешит перейти к менее сухим материям из следующей главы, может пропустить его (а также часть более трудных упражнений к § 4) при первом чтении.

Предложение. *Существует ровно одно неразветвленное расширение K_f^{unram} поля $\mathbb{Q}_p$ степени f, и оно может быть получено присоединением примитивного корня степени $p^f - 1$ из 1. Пусть K — некоторое расширение поля $\mathbb{Q}_p$ степени n с индексом ветвления e и степенью поля вычетов f (так что $n = ef$, как это будет доказано ниже в упр. 12). Тогда $K = K_f^{\mathrm{unram}}(\pi)$, где π — корень некоторого многочлена Эйзенштейна с коэффициентами в K_f^{unram}.*

Доказательство. Пусть $\bar{\alpha}$ — образующая мультипликативной группы $\mathbb{F}_{p^f}^\times$ (см. предложение в конце § 1), а $\bar{P}(x) = x^f + \bar{a}_1 x^{f-1} + \ldots + \bar{a}_f$ — ее минимальный многочлен над $\mathbb{F}_p$ (см. упр. 5 к § 1), где $\bar{a}_i \in \mathbb{F}_p$. Для каждого i выберем произвольный элемент $a_i \in \mathbb{Z}_p$ из класса $\bar{a}_i \pmod p$. Положим $P(x) = x^f + a_1 x^{f-1} + \ldots + a_f$. Оче-

видно, $P(x)$ неприводим над $\mathbb{Q}_p$, так как иначе его можно было бы записать в виде произведения двух многочленов с коэффициентами в $\mathbb{Z}_p$, что при редукции по модулю p дало бы разложение в произведение для $\bar{P}(x)$. Пусть $\alpha \in \mathbb{Q}_p^{\text{alg cl}}$ — некоторый корень многочлена $P(x)$, $\tilde{K} = \mathbb{Q}_p(\alpha)$, $\tilde{A} = \{x \in K \mid |x|_p \leqslant 1\}$, $\tilde{M} = \{x \in K \mid |x|_p < 1\}$. Тогда $[\tilde{K} : \mathbb{Q}_p] = f$, в то время как класс смежности $\alpha + \tilde{M}$ является корнем неприводимого над $\mathbb{F}_p$ многочлена $\bar{P}(x)$ степени f. Следовательно, $[\tilde{A}/\tilde{M} : \mathbb{F}_p] = f$ и $\tilde{K}$ — неразветвленное расширение степени f. (Его единственность еще не доказана.)

Предположим теперь, что K — некоторое расширение из второй части данного предложения. Пусть $A = \{x \in K \mid |x|_p \leqslant 1\}$ — кольцо нормирования для $|\ |_p$ в K, а $M = \{x \in K \mid |x|_p < 1\}$ — максимальный идеал в A, так что $A/M = \mathbb{F}_{p^f}$. Рассмотрим $\bar{\alpha} \in \mathbb{F}_{p^f}$, образующую мультипликативной группы $\mathbb{F}_{p^f}^{\times}$. Пусть $\alpha_0 \in A$ — элемент, редуцирующийся в класс $\bar{\alpha} \pmod M$. И, наконец, пусть $\pi \in K$ — произвольный элемент с $\operatorname{ord}_p \pi = 1/e$. Таким образом, $M = \pi A$.

Утверждается, что существует элемент $\alpha \equiv \alpha_0 \pmod \pi$, для которого $\alpha^{p^f - 1} - 1 = 0$. Доказывается это аналогично лемме Гензеля. А именно, пусть $\alpha \equiv \alpha_0 + \alpha_1 \pi \pmod{\pi^2}$. Тогда выполнено сравнение $0 \equiv (\alpha_0 + \alpha_1\pi)^{p^f - 1} - 1 \equiv \alpha_0^{p^f - 1} - 1 + (p^f - 1)\alpha_1 \pi \alpha_0^{p^f - 2} \equiv \alpha_0^{p^f - 1} - 1 - \alpha_1 \pi \alpha_0^{p^f - 2} \pmod{\pi^2}$. Но $\alpha_0^{p^f - 1} \equiv 1 \pmod \pi$, поэтому $\alpha_1 \equiv \left(\alpha_0^{p^f - 1} - 1\right)/\left(\pi \alpha_0^{p^f - 2}\right) \pmod \pi$ удовлетворяет нужному сравнению по модулю π^2. Продолжая этот процесс вычисления далее, как и в лемме Гензеля, мы находим $\alpha = \alpha_0 + \alpha_1 \pi + \alpha_2 \pi^2 + \ldots$, решение уравнения $\alpha^{p^f - 1} = 1$.

Отметим, что $\alpha, \alpha^2, \ldots, \alpha^{p^f - 1}$ — различные элементы, потому что различны их редукции $\bar{\alpha}, \bar{\alpha}^2, \ldots, \bar{\alpha}^{p^f - 1}$ по модулю M. Иначе говоря, α — примитивный корень степени $p^f - 1$ из 1. Кроме того, $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] \geqslant f$, так как f — степень расширения поля вычетов. (Вскоре мы увидим, что $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = f$.)

Предыдущее рассуждение применимо, в частности, к полю $\tilde{K}$, построенному в первом абзаце доказательства. Следовательно, $\tilde{K} \supset \mathbb{Q}_p(\alpha)$, где α — примитивный корень степени $p^f - 1$ из 1. В силу неравенств $f = [\tilde{K} : \mathbb{Q}_p] \geqslant [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] \geqslant f$ получаем, что $\tilde{K} = \mathbb{Q}_p(\alpha)$. Значит, неразветвленное расширение степени f единственно. Обозначим его через K_f^{unram}.

Вернемся к нашему полю K степени $n = ef$ над $\mathbb{Q}_p$. Пусть $E(x)$ — минимальный многочлен элемента π над $\tilde{K} = K_f^{\text{unram}}$. Обозначим через $\{\pi_i\}$ множество всех элементов, сопряженных с π над K_f^{unram}, так что $E(x) = \prod (x - \pi_i)$. Пусть d — степень, а c — постоянный член $E(x)$. Тогда $\operatorname{ord}_p c = d \operatorname{ord}_p \pi = d/e$. Но поскольку $ef = n = [K : \mathbb{Q}_p] = [K : K_f^{\text{unram}}][K_f^{\text{unram}} : \mathbb{Q}_p] = [K : K_f^{\text{unram}}] \cdot f$, то $d \leqslant e$. С другой стороны, порядок $\operatorname{ord}_p c$ цел, так как $c \in K_f^{\text{unram}}$. Отсюда мы заключаем, что $d = e$ и $\operatorname{ord}_p c = 1$. Таким образом, $E(x)$ — многочлен Эйзенштейна и $K = K_f^{\text{unram}}(\pi)$. □

Следствие. *Пусть K — конечное расширение поля $\mathbb{Q}_p$ степени n с индексом ветвления e и полем вычетов степени f, а π — такой элемент, что $\operatorname{ord}_p \pi = 1/e$. Тогда каждый элемент $\alpha \in K$ однозначно представим в виде*

$$\sum_{i=m}^{\infty} a_i \pi^i,$$

где $m = e \operatorname{ord}_p \alpha$, а каждое a_i удовлетворяет уравнению $a_i^{p^f} = a_i$ (т. е. a_i — представители Тейхмюллера).

Доказательство этого следствия несложно, и мы оставляем его читателю.

Для всякого целого положительного m, не делящегося на p, можно найти степень p^f числа p, сравнимую с 1 по модулю m (действительно, пусть, например, f — порядок мультипликативной группы вычетов $(\mathbb{Z}/m\mathbb{Z})^\times$ по модулю m целых чисел, взаимно простых с m). Тогда $p^f - 1 = mm'$, и если к полю $\mathbb{Q}_p$ присоединить примитивный корень α из 1 степени $p^f - 1$, то в полученном поле элемент $\alpha^{m'}$ будет примитивным

корнем из 1 степени m. Из этого можно заключить, что *конечные неразветвленные расширения поля* $\mathbb{Q}_p$ — *это в точности все расширения, полученные присоединением корней из* 1 *степени, взаимно простой с* p.

Объединение всех конечных неразветвленных расширений поля $\mathbb{Q}_p$ обозначается $\mathbb{Q}_p^{\mathrm{unram}}$ и называется *максимальным неразветвленным расширением поля* $\mathbb{Q}_p$. Кольцо целых $\mathbb{Z}_p^{\mathrm{unram}}$ поля $\mathbb{Q}_p^{\mathrm{unram}}$ (также называемое *кольцом нормирования*) есть

$$\mathbb{Z}_p^{\mathrm{unram}} \underset{\text{def}}{=} \left\{x \in \mathbb{Q}_p^{\mathrm{unram}} \mid |x|_p \leqslant 1\right\}.$$

Оно имеет (единственный) максимальный идеал $M^{\mathrm{unram}} = p\mathbb{Z}_p^{\mathrm{unram}} = \left\{x \in \mathbb{Q}_p^{\mathrm{unram}} \mid |x|_p < 1\right\} = \left\{x \in \mathbb{Q}_p^{\mathrm{unram}} \mid |x|_p \leqslant 1/p\right\}$. Очевидно, поле вычетов $\mathbb{Z}_p^{\mathrm{unram}}/p\mathbb{Z}_p^{\mathrm{unram}}$ есть алгебраическое замыкание $\bar{\mathbb{F}}_p$ поля $\mathbb{F}_p$. Каждый $\bar{x} \in \bar{\mathbb{F}}_p$ обладает единственным *представителем Тейхмюллера* $x \in \mathbb{Z}_p^{\mathrm{unram}}$, который является корнем из 1 с образом $\bar{x}$ в $\mathbb{Z}_p^{\mathrm{unram}}/p\mathbb{Z}_p^{\mathrm{unram}}$. По этой причине $\mathbb{Z}_p^{\mathrm{unram}}$ часто называют «поднятием $\bar{\mathbb{F}}_p$ в характеристику нуль» (а также *кольцом векторов Витта поля* $\bar{\mathbb{F}}_p$).

Поле $\mathbb{Q}_p^{\mathrm{unram}}$, гораздо меньшее, чем $\mathbb{Q}_p^{\mathrm{algcl}}$, во многих ситуациях может использоваться вместо $\mathbb{Q}_p^{\mathrm{algcl}}$.

«Противоположный» к неразветвленным расширениям класс образуют вполне разветвленные расширения. Такое расширение можно построить, например, присоединением примитивного корня из 1 степени p^r; при этом получается вполне разветвленное расширение степени $n = e = p^{r-1}(p-1)$ (см. ниже упр. 7). Однако, к сожалению, далеко не все вполне разветвленные расширения задаются присоединением корня из 1. Например, присоединяя корень многочлена $x^m - p$, мы, очевидно, получаем вполне разветвленное расширение K степени m, и если бы K содержалось в поле, заданном присоединением примитивного корня из 1 степени p^r, то число m должно было бы делить $p^{r-1}(p-1)$, что невозможно, скажем, при $m > p$ и $p \nmid m$. Почти все, что мы можем сказать о вполне разветвленных расши-

рениях, содержится в первом предложении данного параграфа и в упр. 14 ниже.

Повторим: расширение K поля $\mathbb{Q}_p$ степени n с индексом ветвления e и степенью поля вычетов f задается присоединением примитивного корня из 1 степени p^f-1 и последующим присоединением к полученному полю K_f^{unram} корня некоторого многочлена Эйзенштейна с коэффициентами в K_f^{unram}.

Закончим этот параграф двумя полезными предложениями.

Предложение (лемма Краснера). *Пусть* $a, b \in \bar{\mathbb{Q}}_p \left(=\mathbb{Q}_p^{\mathrm{alg\,cl}}\right)$. *Предположим, что элемент* b *расположен к* a *ближе, чем любой из сопряженных* a_i $(a_i \neq a)$ *для этого* a, *т. е.*

$$|b-a|_p < |a_i-a|_p.$$

Тогда $\mathbb{Q}_p(a) \subset \mathbb{Q}_p(b)$.

Доказательство. Пусть $K=\mathbb{Q}_p(b)$. Предположим, что $a \notin K$. Тогда имеется $[K(a):K]>1$ элементов, сопряженных с a *над* K. Следовательно, существует по крайней мере одно $a_i \notin K$, $a_i \neq a$, а также изоморфизм σ поля $\mathbb{Q}_p(a)$ в $\mathbb{Q}_p(a_i)$, оставляющий на месте все элементы K и переводящий a в a_i. Мы уже знаем, что $|\sigma x|_p = |x|_p$ для любого $x \in K(a)$ в силу единственности продолжения нормы. В частности, $|b-a_i|_p = |\sigma b - \sigma a|_p = |b-a|_p$, откуда следует неравенство

$$|a_i-a|_p \leqslant \max\left(|a_i-b|_p,\ |b-a|_p\right) = |b-a|_p < |a_i-a|_p,$$

противоречащее предположению. □

Отметим, что точно таким же методом лемму Краснера можно доказать в более общей формулировке: если $a, b \in \bar{\mathbb{Q}}_p$, K — конечное расширение поля $\mathbb{Q}_p$ и $|b-a|_p < |a_i-a|_p$ для всех a_i, сопряженных с a *над* K $(a_i \neq a)$, то $K(a) \subset K(b)$.

Рассмотрим теперь произвольное поле K с нормой $\|\ \|$. Пусть $f, g \in K[X]$, т. е. $f=\sum a_i X^i$ и $g=\sum b_i X^i$ — два многочлена с коэффициентами в K. Определим рас-

стояние $\|f-g\|$ от f до g как

$$\|f-g\| \underset{\text{def}}{=} \max_i \|a_i - b_i\|.$$

Предложение. *Пусть K — конечное расширение поля $\mathbb{Q}_p$, а $f(X) \in K[X]$ — многочлен степени n,*

$$f(X) = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0.$$

Предположим, что все корни f в $\overline{\mathbb{Q}}_p$ различны. Тогда для любого (достаточно малого) $\varepsilon > 0$ существует такое δ, что если многочлен $g = \sum_{i=0}^{n} b_i X^i \in K[X]$ имеет степень n и $|f-g|_p < \delta$, то для каждого корня α_i многочлена $f(X)$ существует в точности один корень β_i многочлена $g(X)$, для которого $|\alpha_i - \beta_i|_p < \varepsilon$.

Доказательство. Если β — корень $g(X)$, то

$$|f(\beta)|_p = |f(\beta) - g(\beta)|_p = \left|\sum_{i=0}^{n} (a_i - b_i)\beta^i\right|_p \leqslant$$

$$\leqslant \max_i \left(|a_i - b_i|_p |\beta|_p^i\right) \leqslant |f-g|_p \max\left(1, |\beta|_p^n\right) < \delta C_1^n$$

для некоторой константы C_1 (см. ниже упр. 3).

Пусть $C_2 = \min\limits_{1 \leqslant i < j \leqslant n} |\alpha_i - \alpha_j|_p$. Очевидно, $C_2 \neq 0$, так как все α_i различны. Тогда неравенство $|\beta - \alpha_i|_p < C_2$ имеет место не более чем для одного α_i (так как если бы оно выполнялось для другого $\alpha_j \neq \alpha_i$, то мы имели бы $|\alpha_i - \alpha_j|_p \leqslant \max(|\alpha_i - \beta|_p, |\beta - \alpha_j|_p) < C_2$). Поскольку

$$C_1^n \delta > |f(\beta)|_p = \left|a_n \prod (\beta - \alpha_i)\right|_p = |a_n|_p \prod |\beta - \alpha_i|_p$$

$\left(\text{так как } f(X) = a_n \prod (X - \alpha_i)\right)$, то при достаточно малом δ такое α_i, для которого $|\beta - \alpha_i|_p < C_2$, существует. Более того, для этого α_i

$$|\beta - \alpha_i|_p < \frac{C_1^n \delta}{|a_n|_p \prod\limits_{j \neq i} |\beta - \alpha_j|_p} \leqslant \frac{C_1^n \delta}{|a_n|_p \cdot C_2^{n-1}},$$

а последнюю величину можно сделать $< \varepsilon$ при подходящем выборе δ. □

До сих пор мы имели дело исключительно с алгебраическими расширениями поля $\mathbb{Q}_p$. Но, как отмечалось выше, для конструкции p-адического аналога поля комплексных чисел этого недостаточно.

Теорема 12. *Поле $\bar{\mathbb{Q}}_p$ не полно.*

Доказательство. Нужно построить пример последовательности Коши $\{a_i\}$ в $\bar{\mathbb{Q}}_p$, которая не сходится ни к какому $a \in \bar{\mathbb{Q}}_p$.

Пусть b_i — примитивный корень из 1 степени $p^{2^i}-1$ в $\bar{\mathbb{Q}}_p$, т. е. $b_i^{p^{2^i}-1}=1$ и $b_i^m \neq 1$ для $0<m<p^{2^i}-1$. Заметим, что $b_i^{p^{2^{i'}}-1}=1$, если $i'>i$, так как $2^i \mid 2^{i'}$ влечет за собой $(p^{2^i}-1)\mid(p^{2^{i'}}-1)$. (На самом деле 2^i можно заменить любой возрастающей последовательностью натуральных чисел, i-й член которой делит $(i+1)$-й, например: 3^i, $i!$ и т. д.) Таким образом, b_i есть степень $b_{i'}$ при $i'>i$. Пусть

$$a_i=\sum_{j=0}^{i} b_j p^{N_j},$$

где $0=N_0<N_1<N_2<\ldots$ — возрастающая последовательность целых положительных чисел, которая будет выбрана позже. Отметим, что b_j при $j=0, 1, \ldots, i$ являются знаками p-адического разложения числа a_i в неразветвленном расширении $\mathbb{Q}_p(b_i)$, так как b_j — представители Тейхмюллера. Последовательность $\{a_i\}$, очевидно, будет последовательностью Коши.

Выберем теперь по индукции подходящие N_j для $j>0$. Предположим, что N_j уже определены для $j \leqslant i$; тогда определено также $a_i=\sum_{j=0}^{i} b_j p^{N_j}$. Пусть $K=\mathbb{Q}_p(b_i)$. В § 3 было доказано, что K есть неразветвленное расширение Галуа степени 2^i. Отметим прежде всего совпадение $\mathbb{Q}_p(a_i)$ с K. В противном случае существовал бы нетривиальный автоморфизм σ поля K, оставляющий a_i на месте (см. пункт (11) § 1). Но $\sigma(a_i)$ имеет

p-адическое разложение $\sum_{j=0}^{i} \sigma(b_j)\, p^{N_j}$ и $\sigma(b_i) \neq b_i$. Поэтому $\sigma(a_i) \neq a_i$, ибо различны их p-адические разложения.

Из упр. 9 к § 1 следует существование такого $N_{i+1} > N_i$, что при $n < 2^i$ и $\alpha_j \in \mathbb{Z}_p$, не делящихся одновременно на p, a_i не удовлетворяет ни одному из сравнений

$$\alpha_n a_i^n + \alpha_{n-1} a_i^{n-1} + \ldots + \alpha_1 a_i + \alpha_0 \equiv 0 \pmod{p^{N_{i+1}}}.$$

Итак, мы построили требуемую последовательность $\{a_i\}$.

Действительно, предположим, что $a \in \overline{\mathbb{Q}}_p$ является пределом этой последовательности. Тогда a удовлетворяет уравнению

$$\alpha_n a^n + \alpha_{n-1} a^{n-1} + \ldots + \alpha_1 a + \alpha_0 = 0,$$

причем можно считать, что $\alpha_i \in \mathbb{Z}_p$ и не делятся одновременно на p. Выберем i, для которого $2^i > n$. Так как $a \equiv a_i \pmod{p^{N_{i+1}}}$, это приводит к противоречию:

$$\alpha_n a_i^n + \alpha_{n-1} a_i^{n-1} + \ldots + \alpha_1 a_i + \alpha_0 \equiv 0 \pmod{p^{N_{i+1}}}.$$

Теорема доказана. □

Заметим, что мы установили неполноту, используя последовательность из $\mathbb{Q}_p^{\mathrm{unram}}$, а не из всего замыкания $\overline{\mathbb{Q}}_p = \mathbb{Q}_p^{\mathrm{alg\,cl}}$.

Перейдем теперь к «залатыванию дыр» и определим новое поле Ω как *пополнение* поля $\overline{\mathbb{Q}}_p$. Строго говоря, следует рассмотреть классы эквивалентности последовательностей Коши в $\overline{\mathbb{Q}}_p$, а затем определить все необходимые структуры на полученном множестве, поступая при этом точно так же, как и при конструкции $\mathbb{Q}_p$ по $\mathbb{Q}$ (или $\mathbb{R}$ по $\mathbb{Q}$, или как при конструкции пополнения *произвольного* метрического пространства). Интуитивный смысл построения Ω заключается в добавлении всех тех чисел, которые должны быть пределами

сходящихся [1]) бесконечных сумм чисел из $\overline{\mathbb{Q}}_p$, например сумм вида, рассмотренного в доказательстве теоремы 12.

Точно так же, как и при переходе от $\mathbb{Q}$ к $\mathbb{Q}_p$, при переходе от $\overline{\mathbb{Q}}_p$ к Ω можно продолжить норму $|\ |_p$ с $\overline{\mathbb{Q}}_p$ до нормы на Ω, положив $|x|_p = \lim\limits_{i\to\infty} |x_i|_p$, где $\{x_i\}$ — некоторая последовательность Коши элементов из $\overline{\mathbb{Q}}_p$, лежащая в классе эквивалентности x (см. § I.4). Как и в случае перехода от $\mathbb{Q}$ к $\mathbb{Q}_p$, нетрудно показать, что на самом деле при $x \neq 0$ этот предел $|x|_p$ равен $|x_i|_p$ для достаточно больших i.

Продолжим также функцию ord_p на Ω:

$$\mathrm{ord}_p x = -\log_p |x|_p.$$

Следующая теорема утверждает, что на этом работа окончена: Ω может служить p-адическим аналогом поля комплексных чисел.

Теорема 13. *Поле* Ω *алгебраически замкнуто.*

Доказательство. Пусть $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$, $a_i \in \Omega$. Мы должны установить существование корня у $f(X)$ в Ω. Для каждого $i = 0, 1, \ldots, n-1$ выберем последовательность $\{a_{ij}\}_j$ элементов поля $\overline{\mathbb{Q}}_p$, сходящуюся к a_i. Пусть $g_j(X) = X^n + a_{n-1,j}X^{n-1} + \ldots + a_{1,j}X + a_{0,j}$, а r_{ij} — корни многочлена $g_j(X)$ $(i = 1, 2, \ldots, n)$. Утверждается, что можно найти такую последовательность индексов i_j $(1 \leqslant i_j \leqslant n)$, $j = 1, 2, 3, \ldots$, для которой $\{r_{i_j, j}\}$ — последовательность Коши. Действительно, предположим, что мы уже имеем $r_{i_j, j}$ и хотим указать следующее $r_{i_{j+1}, j+1}$. Пусть $\delta_j = |g_j - g_{j+1}|_p = \max\limits_i (|a_{i,j} - a_{i,j+1}|_p)$ (это число стремится к 0 при $j \to \infty$). Положим $A_j = \max(1, |r_{i_j, j}|_p^n)$. Очевидно, существует некоторая константа A, такая, что $A_j \leqslant A$ для всех j (см. ниже упр. 3). Тогда

$$\prod_i |r_{i_j, j} - r_{i, j+1}|_p = |g_{j+1}(r_{i_j, j})|_p = \\ = |g_{j+1}(r_{i_j, j}) - g_j(r_{i_j, j})|_p \leqslant \delta_j A.$$

[1]) В смысле Коши. — *Прим. перев.*

Следовательно, по крайней мере одно из чисел $|r_{i_j,\,j} - r_{i,\,j+1}|_p$ слева $\leqslant \sqrt[n]{\delta_j A}$. Пусть $r_{i_{j+1},\,j+1}$ — соответствующее $r_{i,\,j+1}$. Построенная последовательность $\{r_{i_j,\,j}\}$, очевидно, является последовательностью Коши.

Пусть теперь $r = \lim\limits_{j\to\infty} r_{i_j,\,j} \in \Omega$. Тогда

$$f(r) = \lim_{j\to\infty} f(r_{i_j,\,j}) = \lim_{j\to\infty} g_j(r_{i_j,\,j}) = 0. \quad \square$$

Резюмируя результаты глав I и III, можно сказать, что мы построили наименьшее алгебраически замкнутое поле Ω, содержащее $\mathbb{Q}$ и полное относительно $|\ |_p$. (Строго говоря, это видно из следующего рассуждения: пусть Ω′ — другое такое поле; так как Ω′ полно, оно должно содержать поле, изоморфное p-адическому пополнению поля $\mathbb{Q}$, которое можно обозначить $\mathbb{Q}_p$; далее, поскольку Ω′ содержит $\mathbb{Q}_p$ и алгебраически замкнуто, оно должно содержать поле, изоморфное алгебраическому замыканию поля $\mathbb{Q}_p$; это замыкание можно обозначить $\overline{\mathbb{Q}}_p$; и, наконец, так как Ω′ содержит $\overline{\mathbb{Q}}_p$ и полно, оно должно содержать поле, изоморфное пополнению $\overline{\mathbb{Q}}_p$, которое можно обозначить Ω. Таким образом, любое поле, обладающее указанными выше свойствами, должно содержать поле, изоморфное Ω. Это объясняется тем, что и пополнение, и алгебраическое замыкание определены однозначно с точностью до изоморфизма.)

Поле Ω следовало бы обозначать через Ω_p, напоминая о простом числе p, от которого зависят все конструкции. Но для краткости индекс p мы опускаем.

Построенное поле Ω — это обширная и прекрасная область, место обитания p-адического анализа.

Упражнения

1. Докажите, что множество всевозможных значений $|\ |_p$ на $\overline{\mathbb{Q}}_p$ состоит из всех рациональных степеней p (лежащих в множестве положительных вещественных чисел). Каково это множество для Ω? Напомним, что функция ord_p продолжается на Ω следующим способом: $\mathrm{ord}_p x = -\log_p |x|_p$ (т. е. чтобы получить $|x|_p$, нужно возвести $1/p$ в эту степень). Каково множество всевозможных значений ord_p на Ω? Докажите, что $\overline{\mathbb{Q}}_p$ и Ω *не* яв-

ляются локально компактными. Это одно из существенных отличий Ω от $\mathbb{C}$, которое локально компактно в архимедовой метрике (обычное расстояние на комплексной плоскости).

2. Что получится, если на Ω определить «эллипс» как множество точек, сумма расстояний которых от двух заданных точек a, $b \in \Omega$ постоянна и равна некоторому фиксированному вещественному числу r? Покажите, что этот «эллипс» является либо объединением двух непересекающихся окружностей, либо пересечением двух окружностей, либо пустым множеством в зависимости от выбора a, b и r. Что будет, если определить «гиперболу» как $\{x \in \Omega \mid |x-a|_p - |x-b|_p = r\}$?

3. Пусть $g(X) = X^n + b_{n-1}X^{n-1} + \ldots + b_1 X + b_0$, $C_0 = |g|_p \overset{\text{def}}{=} \max_i |b_i|_p$. Докажите существование такой константы C_1, зависящей только от C_0, что любой корень β многочлена $g(X)$ удовлетворяет неравенству $|\beta|_p < C_1$.

4. Пусть α — корень многочлена $f(X) \in K[X]$ со старшим коэффициентом 1, где K — конечное расширение поля $\mathbb{Q}_p$. Докажите существование такого $\varepsilon > 0$, что всякий полином $g(X)$ такой же степени, как и f, удовлетворяющий неравенству $|f-g|_p < \varepsilon$, имеет корень β, для которого $K(\alpha) = K(\beta)$.

5. Докажите, что всякое конечное расширение K поля $\mathbb{Q}_p$ содержит конечное расширение F поля рациональных чисел $\mathbb{Q}$, для которого $[F:\mathbb{Q}] = [K:\mathbb{Q}_p]$ и F *плотно* в K, т. е. для каждого элемента $x \in K$ и любого $\varepsilon > 0$ существует $y \in F$ с $|x-y|_p < \varepsilon$.

6. Пусть p — такое простое число, что -1 не имеет квадратного корня в $\mathbb{Q}_p$ (см. упр. 8 к § 1). Используя лемму Краснера, найдите ε, для которого $\mathbb{Q}_p(\sqrt{-a}) = \mathbb{Q}_p(\sqrt{-1})$ при любом a с $|a-1|_p < \varepsilon$. Для какого ε из неравенства $|a-p|_p < \varepsilon$ следует совпадение $\mathbb{Q}_p(\sqrt{a})$ с $\mathbb{Q}_p(\sqrt{p})$? (Отдельно исследуйте случай $p=2$.)

7. Пусть a — примитивный корень из 1 степени p^n в $\overline{\mathbb{Q}}_p$, т. е. $a^{p^{n-1}} \neq 1$. Найдите $|a-1|_p$. (*Указание*: a имеет минимальный многочлен $(X^{p^n}-1)/(X^{p^{n-1}}-1)$; при $n=1$ см. упр. 14 к § I.5.) Пусть $n=1$. Докажите, что $\mathbb{Q}_p(a) = \mathbb{Q}_p((-p)^{1/(p-1)})$. Докажите, что если a — примитивный корень из 1 степени m и m не равно степени числа p, то $|a-1|_p = 1$.

8. Пусть K — конечное расширение поля $\mathbb{Q}_p$, m — некоторое целое положительное число, а $(K^\times)^m$ обозначает множество m-х степеней элементов из $K^\times$. Предположим, что: (1) $|m|_p = 1$ и (2) K не содержит корней степени m из 1, отличных от 1. (Например, для $K = \mathbb{Q}_p$ легко проверить, что эти два условия выполнены тогда и только тогда, когда m взаимно просто с p и $p-1$.) Докажите, что индекс мультипликативной подгруппы $(K^\times)^m$ в $K^\times$ (т. е. число различных классов смежности) равен m.

9. Опустим оба предположения предыдущего упражнения. Докажите, что индекс $(K^\times)^m$ в $K^\times$ равен $m\omega/|m|_p$, где ω — число корней из 1 степени m, содержащихся в поле K.

10. Пусть K — вполне разветвленное расширение поля $\mathbb{Q}_p$. Покажите, что каждый корень степени m из 1 в поле K лежит на самом деле в $\mathbb{Q}_p$, если p не делит m.

11. Определите мощность множеств $\mathbb{Q}_p$, $\overline{\mathbb{Q}}_p$ и Ω.

12. Докажите, что $ef=n$, где $n=[K:\mathbb{Q}_p]$, e — индекс ветвления, а f — степень поля вычетов. (*Указание.* Пусть $y_1, \ldots, y_f$ — элементы поля K, для которых $|y_i|_p=1$, а их образы в поле вычетов составляют базис этого поля над $\mathbb{F}_p$. Покажите, что $y_i\pi^j$, $1\leqslant i\leqslant f$, $0\leqslant j\leqslant e-1$, составляют базис в K над $\mathbb{Q}_p$, где $\operatorname{ord}_p\pi=1/e$.)

13. Пусть K — вполне разветвленное расширение степени e поля $\mathbb{Q}_p$. Установите существование такого $\beta\in K$, что $|\beta^e-\alpha|_p<1/p$ для некоторого $\alpha\in\mathbb{Z}_p$ с $\operatorname{ord}_p\alpha=1$

14. Предположим, что K — *ручное* вполне разветвленное расширение. Используя метод леммы Гензеля, покажите, что найденное выше β можно подправить так, чтобы для него было справедливо включение $\beta^e\in\mathbb{Q}_p$, т. е. β удовлетворяло уравнению $X^e-\alpha=0$, где $\alpha\in\mathbb{Z}_p$ и $\operatorname{ord}_p\alpha=1$. Заметим, что тогда $K=\mathbb{Q}_p(\beta)$ (объясните почему).

15. Докажите для любого натурального n конечность числа расширений поля $\mathbb{Q}_p$ степени, не превосходящей n.

16. Комплексных чисел гораздо больше, чем рациональных и даже алгебраических, потому что два последних множества счетны, а $\mathbb{C}$ имеет мощность континуума. Поле Ω также много больше, чем $\mathbb{Q}_p^{\text{alg cl}}$, хотя и в другом смысле (см. выше упр. 11). Докажите, что Ω нельзя представить в виде алгебраического расширения поля, полученного присоединением счетного числа элементов поля Ω к $\overline{\mathbb{Q}}_p$ (т. е. поля, состоящего из всех рациональных выражений от этих элементов и элементов поля $\overline{\mathbb{Q}}_p$). Можно сказать, что Ω имеет *несчетную степень трансцендентности над* $\overline{\mathbb{Q}}_p$. (*Предупреждение.* Это упражнение и следующее — трудные!

17. Будет ли счетной степень трансцендентности Ω над p-адическим пополнением поля $\mathbb{Q}_p^{\text{unram}}$?

Глава IV

p-АДИЧЕСКИЕ СТЕПЕННЫЕ РЯДЫ

§ 1. ЭЛЕМЕНТАРНЫЕ ФУНКЦИИ

Напомним, что в метрическом пространстве, метрика которого индуцирована некоторой неархимедовой нормой $\| \ \|$, последовательность удовлетворяет условию Коши в том и только том случае, когда разность между ее соседними членами стремится к нулю. Более того, если это метрическое пространство полно, бесконечная сумма в нем сходится тогда и только тогда, когда ее общий член стремится к нулю. Поэтому выражения вида

$$f(X)=\sum_{n=0}^{\infty} a_n X^n, \quad a_n \in \Omega,$$

позволяют задать значение функции $f(x)$ как $\sum_{n=0}^{\infty} a_n x^n$ для всех тех значений $x \in \Omega$ переменной X, для которых $|a_n x^n|_p \to 0$.

Следуя архимедову случаю (степенных рядов над $\mathbb{R}$ или $\mathbb{C}$), определим *радиус сходимости* соотношением

$$r=\frac{1}{\limsup |a_n|_p^{1/n}},$$

где выражение $1/r=\limsup |a_n|_p^{1/n}$ обозначает *наименьшее* вещественное число $1/r$, для которого при *любом* $C>1/r$ существует лишь конечное число величин $|a_n|_p^{1/n}$, больших C. Иначе говоря, $1/r$ есть наибольшая *точка накопления*, т. е. наибольшее вещественное число, представимое в виде предела некоторой подпоследовательности из $\{|a_n|_p^{1/n}\}$. Так, например, $1/r$ равно $\lim\limits_{n\to\infty} |a_n|_p^{1/n}$, если последний предел существует.

Чтобы обосновать употребление термина «радиус сходимости», покажем, что соответствующий ряд сходится при $|x|_p < r$ и расходится при $|x|_p > r$. Пусть сначала $|x|_p < r$. Тогда, положив $|x|_p = (1-\varepsilon)r$, получим $|a_n x^n|_p = \left(r\,|a_n|_p^{1/n}\right)^n (1-\varepsilon)^n$. Так как $|a_n|_p^{1/n} > 1/(r - {}^1/_2\varepsilon r)$ только для конечного числа значений n, то

$$\lim_{n\to\infty} |a_n x^n|_p \leqslant \lim_{n\to\infty} \left(\frac{(1-\varepsilon)\,r}{(1-{}^1/_2\varepsilon)\,r}\right)^n = \lim_{n\to\infty} \left(\frac{1-\varepsilon}{1-{}^1/_2\varepsilon}\right)^n = 0.$$

Если $|x|_p > r$, то подобным же образом легко установить, что $a_n x^n$ не стремится к 0 при $n \to \infty$.

Что происходит при $|x|_p = r$? В архимедовом случае ряды могут вести себя довольно сложно на границе интервала или круга сходимости. Например, $\log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} x^n/n$ имеет радиус сходимости 1. При $|x| = 1$ этот ряд расходится для $x = -1$ и сходится (*условно*, не абсолютно) для всех остальных значений x (т. е. для $x = 1$ в вещественном случае и во всех точках единичной окружности, исключая $x = -1$, в комплексном).

В неархимедовом же случае ответ не зависит от точки границы $|x|_p = r$. Это происходит по той причине, что в данной ситуации ряд сходится тогда и только тогда, когда его члены стремятся к нулю, т. е. тогда и только тогда, когда $|a_n|_p |x|_p^n \to 0$. Но это условие зависит только от нормы $|x|_p$, а не от конкретного значения x с заданной нормой. Такого явления, как условная сходимость, здесь просто не существует (ряд $\sum \pm a_n$ сходится или расходится независимо от выбора знаков $\pm$).

Если мы рассмотрим тот же пример $\sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$, то найдем, что $|a_n|_p = p^{\operatorname{ord}_p n}$ и $\lim_{n\to\infty} |a_n|_p^{1/n} = 1$. Поэтому этот ряд сходится при $|x|_p < 1$ и расходится при $|x|_p > 1$. Когда $|x|_p = 1$, $|a_n x^n|_p = p^{\operatorname{ord}_p n} \geqslant 1$ и ряд расходится для всех таких x.

Введем теперь некоторые обозначения. Пусть R — кольцо. Обозначим через $R[[X]]$ кольцо формальных степенных рядов от X с коэффициентами в R, т. е. множество выражений $\sum_{n=0}^{\infty} a_n X^n$, $a_n \in R$, которые складываются и умножаются по обычным правилам. Обычно в дальнейшем R будет одним из следующих колец: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_p$, $\mathbb{Q}_p$ или Ω. Это обозначение часто используется для компактной записи других множеств, например:

$$1+XR[[X]] \overset{\text{def}}{=} \{f \in R[[X]] \mid \text{постоянный член } a_0 \text{ ряда } f \text{ равен } 1\}.$$

Множество

$$D_a(r) \overset{\text{def}}{=} \{x \in \Omega \mid |x-a|_p \leqslant r\}$$

называется *замкнутым диском радиуса* $r \in \mathbb{R}$ *с центром в точке* $a \in \Omega$, а

$$D_a(r^-) \overset{\text{def}}{=} \{x \in \Omega \mid |x-a|_p < r\}$$

— *открытым диском радиуса* r *с центром в* a. Кроме того, положим $D(r) \overset{\text{def}}{=} D_0(r)$ и $D(r^-) \overset{\text{def}}{=} D_0(r^-)$. (Замечание: сразу оговоримся, что ниже, говоря о замкнутом диске $D(r)$ из Ω, мы всегда подразумеваем, что r — одно из возможных значений $|\ |_p$, т. е. рациональная степень числа p; в противном случае, когда не существует $x \in \Omega$ с $|x|_p = r$, мы всегда пишем $D(r^-)$.)

(Предостережение. Термины «открытый» и «замкнутый» введены лишь по аналогии с архимедовым случаем. С топологической точки зрения такая терминология неудачна. А именно, множество $C_c = \{x \in \Omega \mid |x-a|_p = c\}$ открыто в топологическом смысле, так как каждая точка $x \in C_c$ обладает открытой окрестностью, например $D_x(c^-)$, все точки которой лежат в C_c. Поэтому любое объединение этих множеств C_c открыто. Оба диска $D_a(r)$ и $D_a(r^-)$, так же как и их дополнения, являются такими объединениями, например $D_a(r^-) = \bigcup_{c<a} C_c$. Следовательно, диски $D_a(r)$ и $D_a(r^-)$ одновременно *открыты и замкнуты*. Топологическое

пространство, подобное Ω, с такими странными свойствами называется *вполне несвязным*.)

Чтобы привыкнуть к обозначениям, докажем следующую тривиальную лемму.

Лемма 1. *Каждый ряд* $f(X) \in \mathbb{Z}_p[[X]]$ *сходится на* $D(1^-)$.

Доказательство. Пусть $f(X) = \sum_{n=0}^{\infty} a_n X^n$, $a_n \in \mathbb{Z}_p$ и $x \in D(1^-)$. Тогда $|x|_p < 1$. Кроме того, $|a_n|_p \leqslant 1$ для всех n. Следовательно, $|a_n x^n|_p \leqslant |x|_p^n \to 0$ при $n \to \infty$. □

Установим еще один простой результат.

Лемма 2. *Каждый ряд* $f(X) = \sum_{n=0}^{\infty} a_n X^n \in \Omega[[X]]$, *сходящийся на некотором (открытом или замкнутом) диске* $D = D(r)$ *или* $D(r^-)$, *непрерывен на* D.

Доказательство. Пусть x — точка в D. Предположим, что $|x' - x|_p < \delta$, где $\delta < |x|_p$ будет выбрано позже. Тогда $|x'|_p = |x|_p$. (Ниже предполагаем, что $x \neq 0$; случай $x = 0$ очень легко проверить отдельно.) Имеем

$$|f(x) - f(x')|_p = \left| \sum_{n=0}^{\infty} (a_n x^n - a_n x'^n) \right|_p \leqslant$$

$$\leqslant \max_n (|a_n x^n - a_n x'^n|_p) = \max_n (|a_n|_p |(x - x')(x^{n-1} + x^{n-2}x' + \ldots + xx'^{n-2} + x'^{n-1}|_p).$$

Но $|x^{n-1} + x^{n-2}x' + \ldots + xx'^{n-2} + x'^{n-1}|_p) \leqslant \max_{1 \leqslant i \leqslant n} |x^{n-i} x'^{i-1}|_p = |x|_p^{n-1}$. Следовательно,

$$|f(x) - f(x')|_p \leqslant \max_n (|x - x'|_p |a_n|_p |x|_p^{n-1}) < \frac{\delta}{|x|_p} \max_n (|a_n|_p |x|_p^n).$$

Так как $|a_n|_p |x|_p^n$ ограничено при $n \to \infty$, то $|f(x) - f(x')|_p < \varepsilon$ для подходящего δ. □

Вернемся к ряду $\sum_{n=1}^{\infty}(-1)^{n+1}X^n/n$, который, как мы уже выяснили, имеет диск сходимости $D(1^-)$. Таким образом, этот ряд задает функцию на $D(1^-)$, принимающую значения в Ω. Обозначим эту функцию $\log_p(1+X)$, где индекс p напомнит нам о простом числе, определяющем норму на $\mathbb{Q}$, по которой строится Ω, а также не даст перепутать эту функцию с классическим логарифмом $\log(1+X)$, имеющим другую область определения (подмножество в $\mathbb{R}$ или $\mathbb{C}$) и область значений ($\mathbb{R}$ или $\mathbb{C}$). К сожалению, обозначение *p-адического логарифма* $\log_p$ совпадает с классическим обозначением для логарифма по основанию p. Начиная с этого места, под $\log_p$ всегда понимается p-адический логарифм

$$\log_p(1+X)\colon D(1^-)\to\Omega, \quad \log_p(1+x)=\sum_{n=1}^{\infty}(-1)^{n+1}x^n/n,$$

если противное не оговорено *явно*.

Ловушки, подстерегающие тех, кто путает архимедовы и p-адические функции, будут проиллюстрированы ниже, а также в упр. 8—10 к § 2.

Все когда-либо изучавшие дифференциальные уравнения (и многие не изучавшие) понимают, что функция $\exp(x)=e^x=\sum_{n=0}^{\infty}x^n/n!$ является, может быть, самой важной в классической математике. Поэтому взглянем на этот ряд $\sum_{n=0}^{\infty}X^n/n!$ p-адически. Классический экспоненциальный ряд сходится всюду благодаря стремительному росту величины $n!$ в знаменателе. Но если в классическом случае большой знаменатель способствует сходимости, в p-адической ситуации он может играть обратную роль. Действительно, нетрудно вычислить (см. упр. 13 к § I.2), что

$$\operatorname{ord}_p(n!)=\frac{n-S_n}{p-1}$$

(S_n = сумма знаков p-ичной записи числа n);

$$|1/n!|_p = p^{(n-S_n)/(p-1)}.$$

Из формулы $r = 1/(\limsup |a_n|_p^{1/n})$ для радиуса сходимости получаем

$$\operatorname{ord}_p r = \liminf\left(\frac{1}{n}\operatorname{ord}_p a_n\right)$$

(где lim inf некоторой последовательности обозначает наименьшую точку накопления). Тогда в случае $a_n = 1/n!$ имеем

$$\operatorname{ord}_p r = \liminf\left(-\frac{n-S_n}{n(p-1)}\right),$$

но $\lim\limits_{n\to\infty}(-(n-S_n)/(n(p-1))) = -1/(p-1)$. Следовательно, $\sum\limits_{n=0}^{\infty} x^n/n!$ сходится при $|x|_p < p^{-1/(p-1)}$ и расходится при $|x|_p > p^{-1/(p-1)}$. Что происходит при $|x|_p = p^{-1/(p-1)}$, т. е. когда $\operatorname{ord}_p x = 1/(p-1)$? В этом случае

$$\operatorname{ord}_p(a_n x^n) = -\frac{n-S_n}{p-1} + \frac{n}{p-1} = \frac{S_n}{p-1}.$$

Если, например, $n = p^m$ — степень p, то $S_n = 1$. Поэтому $\operatorname{ord}_p\left(a_{p^m}x^{p^m}\right) = 1/(p-1)$, $|a_{p^m}x^{p^m}|_p = p^{-1/(p-1)}$ и $a_n x^n$ не стремится к 0 при $n\to\infty$. Итак, $\sum\limits_{n=0}^{\infty} X^n/n!$ имеет диск сходимости $D(p^{-1/(p-1)-})$ (последний минус, как обычно, обозначает открытый диск). Положим $\exp_p(X) \underset{\text{def}}{=} \sum\limits_{n=0}^{\infty} X^n/n! \in \mathbb{Q}_p[[X]]$. Отметим, что $D(p^{-1/(p-1)-}) \subset D(1^-)$. Поэтому $\exp_p$ сходится в *меньшем* диске, чем $\log_p$!

Несмотря на важные различия между log (exp) и $\log_p$ ($\exp_p$), о которых никогда не следует забывать, некоторые из основных свойств log и exp переносятся на p-адический случай. Установим, например, основное свойство логарифма: логарифм произведения равен сумме логарифмов сомножителей. Прежде всего заме-

тим, что если $x \in D(1^-)$, $y \in D(1^-)$, то $(1+x)(1+y) = 1+(x+y+xy) \in 1+D(1^-)$. Таким образом,

$$\log_p[(1+x)(1+y)] = \sum_{n=1}^{\infty} (-1)^{n+1}(x+y+xy)^n/n.$$

Но в кольце формальных степенных рядов от *двух* переменных над $\mathbb{Q}$ (оно обозначается $\mathbb{Q}[[X, Y]]$) выполнено соотношение

$$\sum (-1)^{n+1}X^n/n + \sum (-1)^{n+1}Y^n/n = \sum (-1)^{n+1}(X+Y+XY)^n/n.$$

Оно вытекает из соотношения $\log(1+x)(1+y) = \log(1+x)+\log(1+y)$, верного для $\mathbb{R}$ и $\mathbb{C}$. Тогда разность между двумя частями доказываемого равенства, скажем $F(X, Y)$, обращается в нуль для всех вещественных значений X и Y из интервала $(-1, 1)$. Поэтому коэффициенты при X^mY^n в $F(X, Y)$ равны нулю для всех m и n.

Этот способ доказательства обращения в нуль формального степенного ряда $F(X, Y)$ типичен для многих последующих рассуждений. Предположим, что некоторое выражение, содержащее формальные степенные ряды от X и Y, например $\log(1+X)$, $\log(1+Y)$ или $\log(1+X+Y+XY)$, тождественно обращается в нуль после подстановки в него вместо переменных вещественных чисел из некоторого интервала. Тогда ряд, полученный приведением подобных членов по X^mY^n, будет иметь лишь нулевые коэффициенты. Мы опускаем детали, так как это общий факт, не связанный непосредственно с p-адическими числами. Если вы не уверены, что смогли бы доказать его самостоятельно, посмотрите упр. 25 к § 2, где даны разъяснения и указания.

Возвращаясь к p-адической ситуации, отметим, что члены любого ряда, сходящегося в Ω, можно поставить в любом порядке и полученный ряд будет сходиться к тому же пределу. (Это легко проверить: ведь условной сходимости в этом случае не бывает.) Итак,

$\log_p[(1+x)(1+y)] = \sum_{n=1}^{\infty}(-1)^{n+1}(x+y+xy)^n/n$ можно переписать как $\sum_{m,\,n=0}^{\infty} c_{m,\,n}x^n y^m$. Но по «формальному тождеству» в $\mathbb{Q}[[X,\ Y]]$ все рациональные числа $c_{m,\,n}$ равны 0, кроме чисел с $n=0$ или $m=0$, а для них $c_{0,\,n}=c_{n,\,0}=(-1)^{n+1}/n$ $(c_{0,\,0}=0)$. Отсюда можно заключить, что

$$\log_p[(1+x)(1+y)] = \sum_{n=1}^{\infty}(-1)^{n+1}x^n/n + \sum_{n=1}^{\infty}(-1)^{n+1}y^n/n = \log_p(1+x)+\log_p(1+y).$$

В качестве следствия этой формулы рассмотрим случай, когда $1+x$ есть корень степени p^m из 1. Тогда $|x|_p<1$ (см. упр. 7 к § III.4) и $p^m\log_p(1+x) = \log_p(1+x)^{p^m} = \log_p 1 = 0$. Следовательно, $\log_p(1+x)=0$.

Точно так же доказывается следующий p-адический вариант известного свойства экспоненты: если $x,\ y \in D(p^{-1/(p-1)-})$, то $x+y \in D(p^{-1/(p-1)-})$ и $\exp_p(x+y) = \exp_p(x)\cdot\exp_p(y)$.

Более того, как и в архимедовом случае, функции $\log_p$ и $\exp_p$ взаимно обратны. Точнее, предположим, что $x \in D(p^{-1/(p-1)-})$. Тогда $\exp_p x = 1+\sum_{n=1}^{\infty} x^n/n!$ и $\operatorname{ord}_p(x^n/n!) > n/(p-1)-(n-S_n)/(p-1) = S_n/(p-1)>0$. Отсюда $\exp_p x - 1 \in D(1^-)$. Рассмотрим

$$\log_p(1+\exp_p x-1) = \sum_{n=1}^{\infty}(-1)^{n+1}(\exp_p x-1)^n/n = \sum_{n=1}^{\infty}(-1)^{n+1}\left(\sum_{m=1}^{\infty}x^m/m!\right)^n\Bigg/n.$$

Этот ряд приводится к виду $\sum_{n=1}^{\infty} c_n x^n$. Но по тем же соображениям, что и выше, в $\mathbb{Q}[[X]]$ имеет место

формальное тождество

$$\sum_{n=1}^{\infty}(-1)^{n+1}\left(\sum_{m=1}^{\infty}X^m/m!\right)^n\Big/n=X,$$

вытекающее из того, что $\log(\exp x)=x$ для поля $\mathbb{R}$ или $\mathbb{C}$. Следовательно, $c_1=1$ и $c_n=0$ при $n>1$, откуда

$$\log_p(1+\exp_p x-1)=x \quad \text{для всех } x\in D(p^{-1/(p-1)}-).$$

Вычисляя выражение $\exp_p(\log_p(1+x))$, нужно быть немного осторожнее. Дело в том, что даже если x принадлежит области сходимости $D(1^-)$ ряда $\log_p(1+X)$, то совсем *необязательно*, чтобы $\log_p(1+x)$ принадлежал области сходимости $D(p^{-1/(p-1)}-)$ ряда $\exp_p(X)$. Это *верно*, если $x\in D(p^{-1/(p-1)}-)$, ибо тогда при $n\geqslant 1$

$$(\operatorname{ord}_p x^n/n)-\frac{1}{p-1}>\frac{n}{p-1}-\operatorname{ord}_p n-\frac{1}{p-1}=\frac{n-1}{p-1}-\operatorname{ord}_p n,$$

а последнее выражение достигает минимума, равного нулю, при $n=1$ и $n=p$. Поэтому $\operatorname{ord}_p\log_p(1+x)\geqslant \geqslant \min\limits_n \operatorname{ord}_p x^n/n>1/(p-1)$. Затем, как и выше, получаем

$$\exp_p(\log_p(1+x))=1+x \quad \text{для всех} \quad x\in D(p^{-1/(p-1)}-).$$

Все установленные нами факты о $\log_p$ и $\exp_p$ можно кратко резюмировать в следующем утверждении.

Предложение. *Функции* $\log_p$ *и* $\exp_p$ *задают взаимно обратные изоморфизмы между мультипликативной группой точек открытого диска радиуса* $p^{-1/(p-1)}$ *с центром в* 1 *и аддитивной группой точек открытого диска радиуса* $p^{-1/(p-1)}$ *с центром в* 0.

(Это означает в точности следующее: $\log_p$ задает взаимно однозначное соответствие между двумя указанными множествами, при котором образ произведения двух чисел равен сумме образов сомножителей, а $\exp_p$ — обратное отображение.)

Этот изоморфизм подобен изоморфизму в вещественном случае между мультипликативной группой положительных вещественных чисел и аддитивной группой

вещественных чисел, который задается взаимно обратными функциями log и exp.

В частности, в силу этого предложения $\log_p$ инъективен на $D_1(p^{-1/(p-1)-})$, т. е. в $D_1(p^{-1/(p-1)-})$ не существует двух чисел с одним и тем же значением $\log_p$. Легко показать, что $D_1(p^{-1/(p-1)-})$ — наибольший диск, для которого это справедливо. В самом деле, $|\zeta-1|_p = p^{-1/(p-1)}$ для примитивного корня ζ степени p из 1 (см. упр. 7 к § III.4), а $\log_p \zeta = 0 = \log_p 1$.

Аналогично определяются функции

$$\sin_p\colon D(p^{-1/(p-1)-}) \to \Omega,$$

$$\sin_p X = \sum_{n=0}^{\infty} (-1)^n X^{2n+1}/(2n+1)!;$$

$$\cos_p\colon D(p^{-1/(p-1)-}) \to \Omega,$$

$$\cos_p X = \sum_{n=0}^{\infty} (-1)^n X^{2n}/(2n)!.$$

Другой тип функций, важных для классической математики, представляют биномиальные разложения $B_a(x) = (1+x)^a = \sum_{n=0}^{\infty} \frac{a(a-1)\dots(a-n+1)}{n!} x^n$. Если $a \in \mathbb{R}$ или $\mathbb{C}$, этот ряд сходится в $\mathbb{R}$ или $\mathbb{C}$ при $|x|<1$ и расходится при $|x|>1$ (кроме случая, когда a — целое неотрицательное число); при $|x|=1$ этот ряд имеет достаточно сложное поведение, зависящее от конкретного значения a.

Определим теперь для каждого $a \in \Omega$ ряд

$$B_{a,p}(X) \overset{\text{def}}{=} \sum_{n=0}^{\infty} \frac{a(a-1)\dots(a-n+1)}{n!} X^n$$

и проанализируем его сходимость. Предположим вначале, что $|a|_p > 1$. Тогда $|a-i|_p = |a|_p$ и норма $|\ |_p$ n-го члена этого ряда равна $|ax^n/n!|_p$. Поэтому при $|a|_p>1$ ряд $B_{a,p}(X)$ имеет область сходимости $D(p^{-1/(p-1)}/|a|_p)$.

Предположим теперь, что $|a|_p \leqslant 1$. В этом случае картина становится более сложной и зависит от a. Мы не будем приводить здесь ее полное описание. Во всяком случае, $|a-i|_p \leqslant 1$ для любого такого a, откуда $|a(a-1)\ldots(a-n+1)x^n/n!|_p \leqslant |x^n/n!|_p$. Поэтому $B_{a,p}(X)$ сходится по крайней мере на $D(p^{-1/(p-1)-})$.

Вскоре нам понадобится более точный результат о сходимости $B_{a,p}(X)$ для $a \in \mathbb{Z}_p$. Утверждается, что тогда $B_{a,p}(X) \in \mathbb{Z}_p[[X]]$ (и, в частности, этот ряд сходится на $D(1^-)$ по лемме 1). Итак, надо показать, что $a(a-1)\ldots(a-n+1)/n! \in \mathbb{Z}_p$. Пусть a_0 — целое положительное число, большее n, для которого $\operatorname{ord}_p(a-a_0) > N$ (подходящее N будет выбрано позже). Тогда $a_0(a_0-1)\ldots(a_0-n+1)/n! = \binom{a_0}{n} \in \mathbb{Z} \subset \mathbb{Z}_p$. Поэтому достаточно установить, что разность между $a_0(a_0-1)\ldots(a_0-n+1)/n!$ и $a(a-1)\ldots(a-n+1)/n!$ для некоторого N имеет $|\ |_p \leqslant 1$. А это следует прямо из непрерывности многочлена $X(X-1)\ldots(X-n+1)$. Таким образом,

$$B_{a,p}(X) \in \mathbb{Z}_p[[X]], \quad \text{если} \quad a \in \mathbb{Z}_p.$$

Возьмем, например, $a = 1/m$, где $m \in \mathbb{Z}$ и $p \nmid m$. Это один из важных случаев, когда $a \in \mathbb{Z}_p$. Пусть $x \in D(1^-)$. Тогда, используя те же соображения, что и при доказательстве тождества $\log_p(1+x)(1+y) = \log_p(1+x) + \log_p(1+y)$, получаем

$$[B_{1/m,p}(x)]^m = 1+x.$$

Таким образом, $B_{1/m,p}(x)$ есть корень степени m из $1+x$ в Ω. (При $p \mid m$ последнее также имеет место, но только для тех значений x, которые лежат в $D(|m|_p\, p^{-1/(p-1)-})$.) Поэтому для обычных рациональных чисел a можно пользоваться сокращенной записью $B_{a,p}(X) = (1+X)^a$.

Но при этом необходима осмотрительность! Как быть, например, со следующим «парадоксом»? Рассмотрим $4/3 = (1+7/9)^{1/2}$; $\operatorname{ord}_7 7/9 = 1$ в $\mathbb{Z}_7$. Поэтому для $x = 7/9$ и $n \geqslant 1$

$$\left| \frac{1/2\,(1/2-1)\ldots(1/2-n+1)}{n!}\, x^n \right|_7 \leqslant \frac{7^{-n}}{|n!|_7} < 1.$$

Следовательно,

$$1 > |(1+{}^7/_9)^{1/2} - 1|_7 = |{}^4/_3 - 1|_7 = |{}^1/_3|_7 = 1.$$

Что стряслось?

Мы чересчур опрометчиво написали ${}^4/_3 = (1+{}^7/_9)^{1/2}$. Как известно, в $\mathbb{R}$ и в $\mathbb{Q}_7$ число ${}^{16}/_9$ имеет два квадратных корня $\pm {}^4/_3$. В $\mathbb{R}$ ряд для $(1+{}^7/_9)^{1/2}$ сходится к ${}^4/_3$, и мы отдаем предпочтение положительному корню. А в $\mathbb{Q}_7$ предпочтение отдается другому корню $-{}^4/_3 = 1 - {}^7/_3$, поскольку он сравним с 1 по модулю 7. Значит, *один и тот же ряд* рациональных чисел

$$\sum_{n=0}^{\infty} \frac{{}^1/_2\,({}^1/_2-1)\ldots({}^1/_2-n+1)}{n!}\left(\frac{7}{9}\right)^n$$

сходится к некоторому рациональному числу как в 7-адической, так и в архимедовой метрике; но те числа, к которым он сходится, различны! Это контрпример к следующей неверной «теореме».

Не-теорема 1. *Пусть* $\sum_{n=1}^{\infty} a_n$ *— сумма рациональных чисел, сходящаяся к некоторому рациональному числу относительно* $|\ |_p$, *а также к некоторому рациональному числу относительно* $|\ |_\infty$. *Тогда рациональные значения этой суммы для двух метрик совпадают.*

Другие «парадоксы» можно найти ниже в упр. 8—10.

§ 2. ЭКСПОНЕНТА АРТИНА—ХАССЕ

Введем теперь одну «элементарную функцию», которая несколько «лучше», чем $\exp_p$, так как имеет больший диск сходимости, и которая часто используется вместо exp, особенно в тех случаях, когда нужна лучшая сходимость, чем только на $D(p^{-1/(p-1)}-)$. Для этого прежде всего разложим в бесконечное произведение обычную экспоненциальную функцию. Это разложение использует функцию Мёбиуса $\mu(n)$, часто встречающуюся в теории чисел. Для $n \in \{1, 2, 3, \ldots\}$

положим

$$\mu(n)=\begin{cases}0, & \text{если } n \text{ делится на полный квадрат натурального числа, большего 1;}\\ (-1)^k, & \text{если } n \text{ равно произведению } k \text{ различных простых чисел.}\end{cases}$$

Таким образом, $1=\mu(1)=\mu(6)=\mu(221)=\mu(1155)$, $0=\mu(9)=\mu(98)$, $-1=\mu(2)=\mu(97)=\mu(30)=\mu(105)$. Основное свойство функции μ заключается в том, что сумма ее значений по всем делителям некоторого целого положительного числа n равна 1, если $n=1$, и 0 в остальных случаях. Действительно, если $n=p_1^{a_1}\dots p_s^{a_s}$ — разложение на простые множители и $s\geqslant 1$, то

$$\sum_{d\mid n}\mu(d)=\sum_{\substack{\text{всевозможные}\\ \varepsilon_i=0 \text{ или } 1,\ i=1,\ \dots,\ s}}\mu\left(p_1^{\varepsilon_1}\dots p_s^{\varepsilon_s}\right)=$$

$$=\sum(-1)^{\sum\varepsilon_i}=(1-1)^s=0.$$

Теперь утверждается, что в $\mathbb{Q}[[X]]$ имеет место формальное тождество

$$\exp(X)=\prod_{n=1}^{\infty}(1-X^n)^{-\mu(n)/n}\underset{\text{def}}{=}\prod_{n=1}^{\infty}B_{-\mu(n)/n}(-X^n).$$

(Сразу отметим, что это бесконечное произведение бесконечных рядов корректно определено (формально), так как n-й ряд в этом произведении начинается с $1-\mu(n)/nX^n$, т. е. не имеет членов со степенью X, меньшей n, кроме постоянного члена 1; поэтому для того, чтобы найти коэффициент для каждой заданной степени X, достаточно перемножить лишь конечное число рядов.) Для доказательства прологарифмируем правую часть. После приведения подобных членов с одинаковой степенью X получим

$$\log\prod_{n=1}^{\infty}(1-X^n)^{-\mu(n)/n}=-\sum_{n=1}^{\infty}\frac{\mu(n)}{n}\log(1-X^n)=$$

$$=\sum_{n=1}^{\infty}\frac{\mu(n)}{n}\sum_{m=1}^{\infty}\frac{X^{nm}}{m}=\sum_{j=1}^{\infty}\left[\frac{X^j}{j}\sum_{n\mid j}\mu(n)\right]$$

(j — прежнее mn). По доказанному выше основному свойству μ последний ряд равен X. Взяв экспоненту от обеих частей, получаем требуемое формальное тождество.

(В этом доказательстве несколько раз неявно использовался принцип, упоминавшийся при обсуждении $\log_p$. Его подробное изложение дано ниже в упр. 25. Согласно этому принципу, манипуляции с формальными степенными рядами как с функциями вещественных переменных законны, если все получающиеся ряды сходятся в некотором интервале около нуля.)

В p-адическом случае, рассматривая произведение $\prod_{n=1}^{\infty}(1-X^n)^{-\mu(n)/n}$, можно выделить все «нежелательные» сомножители. Под «нежелательными» подразумеваются сомножители, сходящиеся только на $D(p^{-1/(p-1)-})$, а не на $D(1^-)$. А именно, пусть $p \mid n$ и n не содержит полного квадрата >1. В этом случае $(1-X^n)^{-\mu(n)/n}$ сходится только для тех значений x, для которых

$$|x^n|_p = |x|_p^n \in D(r^-),$$

где

$$r = p^{-1/(p-1)}\left(\left|-\frac{\mu(n)}{n}\right|_p\right)^{-1} = p^{-1/(p-1)}\,|n|_p.$$

Например, если $n=p$, сходимость имеет место в точности тогда, когда

$$|x|_p < \left(p^{-1/(p-1)}\,\frac{1}{p}\right)^{1/p} = p^{-1/(p-1)}.$$

До тех пор пока $p \nmid n$, все в порядке, т. е. $(1-X^n)^{-\mu(n)/n} \in \mathbb{Z}_p[[X]]$, так как $-\mu(n)/n \in \mathbb{Z}_p$. (Напомним, что здесь и ниже $(1-X^n)^a$ — всего лишь краткое обозначение для $B_{a,p}(-X^n) = \sum_{i=0}^{\infty} a(a-1)\ldots(a-i+1)(-X^n)^i/i!$.)

Поэтому определим новую функцию E_p, которую называют *экспонентой Артина — Хассе*, опуская все «плохие» сомножители в рассматриваемом бесконечном произведении (это похоже на отбрасывание эйлерова

множителя при определении p-адической дзета-функции в гл. II):

$$E_p(X) \underset{\text{def}}{=} \prod_{\substack{n=1 \\ p \nmid n}}^{\infty} (1-X^n)^{-\mu(n)/n} \in \mathbb{Q}[[X]].$$

Так как каждый ряд $B_{-\mu(n)/n,\,p}(-X^n)$ принадлежит $1+X^n\mathbb{Z}_p[[X]]$, их бесконечное произведение определено (для того чтобы получить коэффициент при заданной степени X, необходимо перемножить лишь конечное число сомножителей) и лежит в $1+X\mathbb{Z}_p[[X]]$.

Легко найти более простое выражение для $E_p(X)$. Для этого воспользуемся следующим свойством функции μ:

$$\sum_{d \mid n,\ p \nmid d} \mu(d) = \begin{cases} 1, & \text{если } n \text{ равно степени } p, \\ 0 & \text{в противном случае.} \end{cases}$$

Это свойство выводится непосредственно из ранее доказанного свойства μ для $n/p^{\operatorname{ord}_p n}$ вместо n. Рассмотрим $E_p(X)$ над $\mathbb{R}$ (или над $\mathbb{C}$). Логарифмируя, мы получим, как и выше:

$$\log E_p(X) = -\sum_{\substack{n=1 \\ p \nmid n}}^{\infty} \frac{\mu(n)}{n} \sum_{m=1}^{\infty} \frac{X^{mn}}{m} =$$

$$= \sum_{j=1}^{\infty} \left[\frac{X^j}{j} \sum_{n \mid j,\ p \nmid n} \mu(n) \right] = \sum_{m=0}^{\infty} \frac{X^{p^m}}{p^m}.$$

Отсюда следует равенство формальных рядов в $\mathbb{Q}[[X]]$:

$$E_p(X) = \exp\left(X + \frac{X^p}{p} + \frac{X^{p^2}}{p^2} + \frac{X^{p^3}}{p^3} + \ldots\right).$$

Важнейшее отличие $E_p(X)$ от $\exp_p(X)$ состоит в том, что $E_p(X) \in \mathbb{Z}_p[[X]]$. Поэтому $E_p(X)$ сходится на

$D(1^-)$. Можно показать (см. упр. 11 к § IV.4), что это в точности диск сходимости, т. е. ряд не сходится на $D(1)$.

В заключение этого параграфа докажем одну полезную общую лемму, принадлежащую Дворку.

Лемма 3. *Пусть* $F(X)=\sum a_iX^i \in 1+X\mathbb{Q}_p[[X]]$. *Тогда* $F(X) \in 1+X\mathbb{Z}_p[[X]]$ *в том и только том случае, когда* $F(X^p)/(F(X))^p \in 1+pX\mathbb{Z}_p[[X]]$.

Доказательство. Пусть $F(X) \in 1+X\mathbb{Z}_p[[X]]$. Тогда из сравнений $(a+b)^p \equiv a^p+b^p \pmod p$ и $a^p \equiv a \pmod p$ для $a \in \mathbb{Z}_p$ следует, что $(F(X))^p = F(X^p)+pG(X)$ при некотором $G(X) \in X\mathbb{Z}_p[[X]]$. Поэтому

$$\frac{F(X^p)}{(F(X))^p} = 1 - \frac{pG(X)}{(F(X))^p} \in 1+pX\mathbb{Z}_p[[X]],$$

так как $(F(X))^p \in 1+X\mathbb{Z}_p[[X]]$, а значит, и обратный к нему ряд лежит в этом же множестве (см. упр. 3).

В другую сторону, пусть

$$F(X^p) = (F(X))^p G(X), \quad G(X) \in 1+pX\mathbb{Z}_p[[X]],$$
$$G(X) = \sum b_iX^i, \qquad F(X) = \sum a_iX^i.$$

Докажем по индукции включение $a_i \in \mathbb{Z}_p$. По предположению $a_0 = 1$. Допустим, что $a_i \in \mathbb{Z}_p$ при $i<n$. Тогда, приравнивая коэффициенты при X^n в обеих частях равенства, получим соотношение

$$\left.\begin{array}{ll} a_{n/p}, & \text{если } p \text{ делит } n \\ 0 & \text{в противном случае} \end{array}\right\} =$$
$$= \text{коэффициент при } X^n \text{ в } \left(\sum_{i=0}^{n} a_iX^i\right)^p \left(1+\sum_{i=1}^{n} b_iX^i\right).$$

Разложим произведение справа по степеням X, а затем вычтем из него $a_{n/p}X^n$, если $p \mid n$ (напомним, что $a_{n/p} \equiv a_{n/p}^p \pmod p$). У полученного многочлена коэффициент при X^n обращается в нуль. С другой стороны, он равен сумме, одно из слагаемых которой есть pa_n,

а остальные принадлежат $p\mathbb{Z}_p$. Отсюда можно заключить, что $pa_n \in p\mathbb{Z}_p$, т. е. $a_n \in \mathbb{Z}_p$. □

Леммой Дворка можно воспользоваться для прямого доказательства (не опирающегося на разложение в бесконечное произведение) того, что все коэффициенты формального степенного ряда $E_p(X) = e^{X+(X^p/p)+(X^{p^2}/p^2)+\ldots}$ лежат в $\mathbb{Z}_p$ (см. ниже упр. 17).

Лемма Дворка, которая на первый взгляд кажется странноватой, в действительности представляет собой образец одного глубокого явления, свойственного p-адическому анализу. Она утверждает, что если известно нечто о $F(X^p)/(F(X))^p$, то известно нечто и о F. Отношение $F(X^p)/(F(X))^p$ измеряет разницу между возведением X в степень p с последующим применением F и между применением F с последующим возведением в степень p, т. е. измеряет, насколько F коммутирует с возведением в p-ю степень. Отображение возведения в степень p играет фундаментальную роль, как мы уже видели в другой p-адической ситуации (ср. с параграфом о конечных полях). Итак, лемма Дворка утверждает, что если F «коммутирует по модулю p» с возведением в степень p, т. е. $F(X^p)/(F(X))^p = 1 + p \cdot \sum(p\text{-адическое целое})X^i$, то F имеет целые p-адические коэффициенты.

Продемонстрируем одно приложение этой леммы к функции, которая нам встретится в доказательстве теоремы Дворка о рациональности дзета-функции. Отметим прежде всего следующее обобщение леммы 3. Пусть $F(X, Y) = \sum a_{m,n} X^n Y^m$ — формальный степенной ряд от *двух* переменных X и Y с постоянным членом 1, т. е.

$$F(X, Y) \in 1 + X\mathbb{Q}_p[[X, Y]] + Y\mathbb{Q}_p[[X, Y]].$$

Тогда все $a_{m,n}$ принадлежат $\mathbb{Z}_p$ в том и только том слчуае, когда

$$F(X^p, Y^p)/(F(X, Y))^p \in \\ \in 1 + pX\mathbb{Z}_p[[X, Y]] + pY\mathbb{Z}_p[[X, Y]].$$

Доказывается это в точности так же, как лемма 3.

Определим теперь ряд $F(X, Y)$ из $\mathbb{Q}[[X, Y]]$ следующим образом:

$$F(X, Y) = B_{X, p}(Y)\, B_{(X^p - X)/p,\, p}(Y^p)\, B_{(X^{p^2} - X^p)/p^2,\, p}(Y^{p^2}) \ldots$$

$$\ldots B_{(X^{p^n} - X^{p^{n-1}})/p^n,\, p}(Y^{p^n}) \ldots =$$

$$= (1+Y)^X (1+Y^p)^{(X^p - X)/p} (1+Y^{p^2})^{(X^{p^2} - X^p)/p^2} \ldots$$

$$\ldots (1+Y^{p^n})^{(X^{p^n} - X^{p^{n-1}})/p^n} \ldots =$$

$$= \sum_{i=0}^{\infty} \frac{X(X-1)\ldots(X-i+1)}{i!} Y^i \times$$

$$\times \prod_{n=1}^{\infty} \left(\sum_{i=0}^{\infty} \frac{X^{p^n} - X^{p^{n-1}}}{p^n} \left(\frac{X^{p^n} - X^{p^{n-1}}}{p^n} - 1 \right) \ldots \right.$$

$$\left. \ldots \left(\frac{X^{p^n} - X^{p^{n-1}}}{p^n} - i + 1 \right) \frac{Y^{ip^n}}{i!} \right).$$

Этот ряд определен корректно, поскольку для того, чтобы найти его коэффициент при любом $X^n Y^m$, достаточно перемножить лишь конечное число сомножителей. Кроме того, ряд $F(X, Y) = \sum a_{m, n} X^n Y^m$ лежит в $1 + X\mathbb{Q}_p[[X, Y]] + Y\mathbb{Q}_p[[X, Y]]$. Используя отмеченное выше обобщение леммы 3, докажем, что $a_{m, n} \in \mathbb{Z}_p$. А именно,

$$\frac{F(X^p, Y^p)}{(F(X, Y))^p} =$$

$$= \frac{(1+Y^p)^{X^p} (1+Y^{p^2})^{(X^{p^2} - X^p)/p} (1+Y^{p^3})^{(X^{p^3} - X^{p^2})/p^2} \ldots}{(1+Y)^{pX} (1+Y^p)^{X^p - X} (1+Y^{p^2})^{(X^{p^2} - X^p)/p} \ldots} =$$

$$= \frac{(1+Y^p)^X}{(1+Y)^{pX}}.$$

Поэтому достаточно показать, что $(1+Y^p)^X/(1+Y)^{pX}$ содержится в $1 + pX\mathbb{Z}_p[[X, Y]] + pY\mathbb{Z}_p[[X, Y]]$. Применив лемму 3 в другом направлении к ряду $1 + Y \in 1 + Y\mathbb{Z}_p[[Y]]$, получим

$$(1+Y^p)/(1+Y)^p = 1 + pYG(Y), \quad G(Y) \in \mathbb{Z}_p[[Y]].$$

Отсюда

$$\frac{(1+Yp)^X}{(1+Y)^{pX}} = (1+pYG(Y))^X = \sum_{i=0}^{\infty} \frac{X(X-1)\dots(X-i+1)}{i!} p^i (YG(Y))^i$$

и последний ряд, очевидно, лежит в $1+pX\mathbb{Z}_p[[X, Y]]+pY\mathbb{Z}_p[[X, Y]]$. Из этого мы заключаем, что $F(X, Y) \in \mathbb{Z}_p[[X, Y]]$.

Упражнения

1. Найдите точный диск сходимости (указывая при этом, замкнут он или открыт) для следующих рядов. (В пунктах (v) и (vi) $\log_p$ обозначает классический логарифм по основанию p; а ζ в (vii) — примитивный корень степени p из 1. Скобки [ ] означают взятие целой части.)

(i) $\sum n!\, X^n$; (iii) $\sum p^n X^n$; (v) $\sum p^{[\log_p n]} X^n$;

(ii) $\sum p^{n[\log n]} X^n$; (iv) $\sum p^n X^{p^n}$; (vi) $\sum p^{[\log_p n]} X^n/n$;

(vii) $\sum (\zeta-1)^n X^n/n!$.

2. Докажите, что если $\sum a_n$ и $\sum b_n$ сходятся соответственно к a и b (где a_i, b_i, a, $b \in \Omega$), то $\sum c_n$ сходится к ab, где $c_n = \sum_{i=0}^{n} a_i b_{n-i}$.

3. Докажите, что элементы множества $1+X\mathbb{Z}_p[[X]]$ образуют группу по умножению. Пусть D — некоторый открытый или замкнутый диск в Ω с центром в 0. Докажите, что множество $\{f \in 1+X\Omega[[X]] \mid f$ сходится на $D\}$ замкнуто относительно умножения, но не является группой. Покажите, что при фиксированном λ множество рядов $f(X) = 1+\sum_{i=1}^{\infty} a_i X^i$, для которых $\operatorname{ord}_p a_i - \lambda i$ больше 0 при всех $i = 1, 2, \dots$ и стремится к ∞ при $i \to \infty$, есть мультипликативная группа. Далее, пусть $f_j \in 1+X\mathbb{Z}_p[[X]]$, $j = 1, 2, 3, \dots$, а $f(X) = \prod_{j=1}^{\infty} f_j(X^j)$. Проверьте включение $f(X) \in 1+X\mathbb{Z}_p[[X]]$. Предположим, что каждое f_j сходится на замкнутом единичном диске $D(1)$. Сходится ли тогда $f(X)$ на $D(1)$ (приведите доказательство или контрпример)? Если все непостоянные коэффициенты для всех f_j делятся на p, то меняется ли от этого ответ (дайте доказательство или контрпример)?

4. Пусть $\{a_n\} \subset \Omega$ — некоторая последовательность и $p^n \mid a_n \mid_p \to 0$. Докажите, что

$$\sum_{n=0}^{\infty} a_n \frac{n!}{x(x+1)(x+2)\ldots(x+n)}$$

сходится при всех $x \in \Omega$, не лежащих в $\mathbb{Z}_p$. Что можно сказать о случае, когда $x \in \mathbb{Z}_p$?

5. Докажите существование, единственность и непрерывность функции f: $\Omega - \{0\} \to \Omega$, для которой

$$f(x) = \log_p x, \text{ если } |x-1|_p < 1; \quad f(p) = 0;$$
$$f(xy) = f(x) + f(y) \quad \text{для всех } x, y \in \Omega - \{0\}.$$

Эта функция называется *логарифмической функцией Ивасавы* и также обозначается через $\log_p$. Покажите, что f нельзя доопределить по непрерывности в 0. (Именно эта функция $\log_p$ уже встречалась нам ранее в формуле для $L_{\chi, p}(1)$ из § II.7.)

6. Пусть i — квадратный корень из -1 в $\overline{\mathbb{Q}}_p$ (на самом деле i лежит в $\mathbb{Q}_p$, если $p \not\equiv 3 \pmod 4$ и $p \neq 2$). Докажите, что $\exp_p(ix) = \cos_p x + i \sin_p x$ для $x \in D(p^{-1/(p-1)-})$.

7. Покажите, что 2-адический порядок рационального числа

$$2 + 2^2/2 + 2^3/3 + 2^4/4 + 2^5/5 + \ldots + 2^n/n$$

стремится к бесконечности с ростом n. Постарайтесь дать хорошую оценку этому 2-адическому порядку в зависимости от n. Можете ли вы придумать полностью элементарное доказательство (без использования p-адического анализа) этого факта, который формулируется совершенно элементарно?

8. Найдите ошибку в следующем «доказательстве» иррациональности числа π, которое слишком прекрасно, чтобы быть верным. Пусть $\pi = a/b$, а $p \neq 2$ — простое число, не делящее a. Тогда

$$0 = \sin(pb\pi) = \sin(pa) = \sum_{n=0}^{\infty} (-1)^n (pa)^{2n+1}/(2n+1)! \equiv pa \pmod{p^2},$$

что невозможно.

9. Найдите ошибку в следующем «доказательстве» трансцендентности e. Предположим, что e алгебраично. Тогда $e-1$ также алгебраично. Возьмем простое число $p \neq 2$, не делящее ни числитель, ни знаменатель никакого коэффициента минимальных многочленов для e и $e-1$ над $\mathbb{Q}$. Тогда $|e|_p = |e-1|_p = 1$. Поэтому $1 = |e-1|_p^p = |(e-1)^p|_p = \left| e^p - 1 - \sum_{i=1}^{p-1} \binom{p}{i} (-e)^i \right|_p$. В последней сумме все биномиальные коэффициенты делятся на p, а $|-e|_p = 1$.

Следовательно, $1=|e^p-1|_p=\left|\sum_{n=1}^{\infty} p^n/n!\right|_p$, что невозможно, так как каждое слагаемое в данной сумме имеет $|\ |_p<1$.

10. (a) Покажите, что биномиальные ряды для $(1-p/(p+1))^{-n}$ (где n — целое положительное рациональное число) и для $(1+(p^2+2mp)/m^2)^{1/2}$ (где m — целое рациональное $>(\sqrt{2}+1)p$ и $p\nmid m$) сходятся к одному и тому же рациональному числу независимо от того, рассматриваем ли мы эту сумму как сумму вещественных или как сумму p-адических чисел.

(b) Пусть $p\geqslant 7$, а $n=(p-1)/2$. Покажите, что $(1+p/n^2)^{1/2}$ дает контрпример к не-теореме 1.

11. Докажите, что для любого целого неотрицательного k p-адическое число $\sum_{n=0}^{\infty} n^k p^n$ лежит в $\mathbb{Q}$.

12. Докажите следующее равенство в $\mathbb{Q}_3$:

$$\sum_{n=1}^{\infty}(-1)^n\frac{3^{2n}}{n4^{2n}}=2\cdot\sum_{n=1}^{\infty}\frac{3^{2n}}{n4^n}.$$

13. Покажите, что диск сходимости степенного ряда $f(X)=\sum a_nX^n$ содержится в диске сходимости формальной производной этого ряда $f'(X)=\sum na_nX^{n-1}$. Постройте пример, в котором эти области сходимости не совпадают.

14. Докажите, что $\exp_p X$, $\sin_p X/X$ и $\cos_p X$ не имеют нулей в своей области сходимости, а $E_p(X)$ не имеет нулей на $D(1^-)$.

15. Найдите коэффициенты ряда $E_p(X)$ при X^i для $i\leqslant 4$ и $p=2$, 3.

16. Найдите коэффициенты всех членов ряда $E_p(X)$ вплоть до X^{p-1}. Найдите также коэффициент при X^p. Какой теореме элементарной теории чисел соответствует тот факт, что коэффициент при X^p лежит в $\mathbb{Z}_p$?

17. Используя лемму Дворка, докажите другим способом, что все коэффициенты ряда $E_p(X)$ принадлежат $\mathbb{Z}_p$.

18. Пусть $f(X)=\exp_p\left(\sum_{i=0}^{\infty} b_iX^{p^i}\right)$, $b_i\in\mathbb{Q}_p$. Используя лемму Дворка, докажите, что $f(X)\in 1+X\mathbb{Z}_p[[X]]$ тогда и только тогда, когда $b_{i-1}-pb_i\in p\mathbb{Z}_p$ для всех $i=0$, 1, 2, ... (где $b_{-1}\overset{\text{def}}{=}0$).

19. (a) Приведите пример бесконечной суммы ненулевых рациональных чисел, которая сходится по норме $|\ |_p$ при *всех* простых p, а также как сумма вещественных чисел (т. е. по норме $|\ |_\infty=|\ |$).

(b) Может ли такая сумма сходиться к некоторому рациональному числу по какой-нибудь из норм $|\ |_p$ или $|\ |_\infty$?

20. Возьмем теперь вместо степенного ряда некоторую функцию $f\colon \Omega \to \Omega$. Копируя известное определение из классического анализа, скажем, что эта функция *дифференцируема* в точке $a \in \Omega$, если существует предел $(f(x)-f(a))/(x-a)$ при $|x-a|_p \to 0$. Пусть $f(X)=\sum_{n=0}^{\infty} a_n X^n$ — некоторый степенной ряд. Докажите прежде всего его дифференцируемость в каждой точке диска сходимости. Кроме того, покажите, что это дифференцирование можно производить почленно, т. е. его производная в каждой точке a диска сходимости равна $\sum_{n=1}^{\infty} n a_n a^{n-1}$. Иначе говоря, ряд, соответствующий производной, совпадает с формальной производной степенного ряда.

21. Используя определение дифференцируемости из предыдущего упражнения, постройте пример всюду дифференцируемой функции $f\colon \Omega \to \Omega$, производная которой тождественно равна 0, а сама эта функция не локально постоянна (подробности о локально постоянных функциях см. в начале § II.3). Более того, эту функцию можно выбрать так, чтобы она обращалась в нуль вместе со всеми производными при $x=0$, но не была постоянной ни в какой окрестности 0. Такая функция подобна замечательной функции e^{-1/x^2} из классического анализа, которая не равна своему ряду Тейлора (тождественно равному нулю) в окрестности начала координат.

22. Теорема о среднем значении из математического анализа в применении к функции $f\colon \mathbb{R} \to \mathbb{R}$, $f(x)=x^p-x$, на интервале $\{x \in \mathbb{R} \mid |x| \leqslant 1\}$ утверждает, что

$$f'(\alpha)=0 \text{ для некоторого } \alpha \in \mathbb{R},\ |\alpha| \leqslant 1,$$

так как $f(1)=f(-1)=0$. (На самом деле $\alpha = \pm (1/p)^{1/(p-1)}$ при $p \neq 2$ и $\alpha = 1/2$ при $p=2$.) Останется ли это верным, если $\mathbb{R}$ заменить на Ω, а $|\ |$ на $|\ |_p$?

23. Определим функцию $f\colon \mathbb{Q}_p \to \mathbb{Q}_p$ сопоставлением $x = \sum a_n p^n \longmapsto \sum g(a_n)\, p^n$, где $\sum a_n p^n$ есть p-адическое разложение числа x, а $g\colon \{0, 1, \ldots, p-1\} \to \mathbb{Q}_p$ — произвольная функция. Докажите непрерывность f. Пусть теперь $g(a)=a^2$, а $p \neq 2$. Докажите, что f *не* дифференцируема.

24. Докажите включение

$$(1+X)^{p^N}-1 \in p^j \mathbb{Z}[X]+X^{p^N-j+1}\mathbb{Z}[X]$$

для любого натурального N и любого $j=1, 2, \ldots, N$. Предположим, что a/b — некоторое рациональное число с $|a/b|_p \leqslant 1$ и мы хотим найти первые M коэффициентов (для достаточного большого M) степенного ряда $(1+X)^{a/b}$ с определенной p-адической точностью. Для решения этой задачи предложите какой-нибудь простой алгоритм (например, программу для ЭВМ). (Все операции

при этом должны выполняться в $\mathbb{Z}/p^n\mathbb{Z}$, а не в $\mathbb{Q}$, так как машинные вычисления обычно гораздо проще производить в первом случае.)

25. Пусть R — некоторое кольцо. Определим кольцо $R[[X_1, \ldots, X_n]]$ (или, короче, $R[[X]]$) формальных степенных рядов от n переменных как множество «последовательностей» $\{r_{i_1, \ldots, i_n}\}$ элементов кольца R, занумерованных наборами n целых неотрицательных чисел $i_1, \ldots, i_n$ (каждая такая последовательность интерпретируется как ряд $\sum r_{i_1, \ldots, i_n} X_1^{i_1} \ldots X_n^{i_n}$ (или, короче, $\sum r_i X^i$), с операциями сложения и умножения, заданными обычным способом. Точнее, $\{r_{i_1, \ldots, i_n}\} + \{s_{i_1, \ldots, i_n}\} = \{t_{i_1, \ldots, i_n}\}$, где $t_{i_1, \ldots, i_n} = r_{i_1, \ldots, i_n} + s_{i_1, \ldots, i_n}$, а $\{r_{i_1, \ldots, i_n}\} \cdot \{s_{i_1, \ldots, i_n}\} = \{t_{i_1, \ldots, i_n}\}$, где $t_{i_1, \ldots, i_n} = \sum r_{j_1, \ldots, j_n} s_{k_1, \ldots, k_n}$, причем суммирование производится по всем парам наборов $j_1, \ldots, j_n$ и $k_1, \ldots, k_n$ с $j_1 + k_1 = i_1$, $j_2 + k_2 = i_2$, $\ldots$, $j_n + k_n = i_n$.

Для каждого ненулевого степенного ряда f определена минимальная степень ненулевых членов $\deg f$: это наименьшее d, для которого существует не равное нулю $r_{i_1, \ldots, i_n}$ с $i_1 + i_2 + \ldots + i_n = d$. Фиксируя некоторое положительное вещественное $\rho < 1$, можно определить на $R[[X]]$ так называемую *X-адическую топологию*, индуцированную *X-адической нормой*

$$|f|_X \underset{\text{def}}{=} \rho^{\deg f} \quad (|0|_X = 0 \text{ по определению}).$$

(1) Покажите, что $|\ |_X$ превращает $R[[X]]$ в неархимедово метрическое пространство (см. самое первое определение в § I.1; под «неархимедовостью» здесь, конечно, понимается выполнение неравенства $d(x, y) \leqslant \max(d(x, z), d(z, y))$, соответствующего третьему свойству нормы). Что означает неравенство $|f|_X < 1$?

(2) Покажите, что $R[[X]]$ полно относительно $|\ |_X$.

(3) Установите, что бесконечное произведение рядов $f_j \in R[[X]]$ сходится тогда и только тогда, когда $|f_j - 1|_X \to 0$ (где 1 обозначает постоянный степенной ряд $\{r_{i_1, \ldots, i_n}\}$ с $r_{0, \ldots, 0} = 1$ и остальными $r_{i_1, \ldots, i_n} = 0$). Поэтому, например, имеет смысл тот ужасный степенной ряд, который определен в конце § 2.

(4) Пусть $f \in R[[X]]$. Обозначим через f_d ряд, полученный из f заменой всех коэффициентов $r_{i_1, \ldots, i_n}$ с $i_1 + \ldots + i_n > d$ на 0. Таким образом, f_d можно считать многочленом от n переменных. Пусть $g_1, \ldots, g_n \in R[[X]]$. Заметим, что $f_d(g_1(X), g_2(X), \ldots, g_n(X))$ определено при любом d, так как это всего лишь конечная сумма произведений степенных рядов. Докажите, что $\{f_d(g_1(X), \ldots, g_n(X))\}_{d=0, 1, 2 \ldots}$ является последовательностью Коши в $R[[X]]$, если $|g_j|_X < 1$ для $j = 1, \ldots, n$. Ее предел в этом случае обозначается через $f \circ g$.

(5) Рассмотрим теперь в качестве R поле вещественных чисел $\mathbb{R}$. Пусть f, f_d, g_1, ..., g_n — такие же ряды, как и в (4), с $|g_j|_X < 1$. Кроме того, предположим, что f и все g_j сходятся абсолютно для всех значений $X_i = x_i$ из интервала $[-\varepsilon, \varepsilon] \subset \mathbb{R}$ при некотором $\varepsilon > 0$. Докажите, что тогда ряд $f \circ g$ сходится абсолютно для всех значений $X_i = x_i$ из (возможно, меньшего) интервала $[-\varepsilon', \varepsilon']$ при некотором $\varepsilon' > 0$.

(6) В предположениях пункта (5) докажите, что $f \circ g$ — нулевой степенной ряд из $\mathbb{R}[[X]]$, если $f \circ g(x_1, \ldots, x_n) = 0$ при любых $x_1, \ldots, x_n \in [-\varepsilon', \varepsilon']$. (*Указание*: прежде всего покажите, что при данных предположениях о сходимости можно переставлять члены встречающихся рядов; затем сведите все к доказательству совпадения с нулевым степенным рядом всякого ряда из $\mathbb{R}[[X]]$, равного нулю при всех значениях переменных из $[-\varepsilon', \varepsilon']$; последнее докажите индукцией по n.)

(7) Пусть $n = 3$. Будем писать X, Y, Z вместо X_1, X_2, X_3. Тогда примером к предыдущему могут служить ряды:

$$f(X, Y, Z) = \sum_{i=1}^{\infty} (-1)^{i+1} \left(\frac{X^i}{i} + \frac{Y^i}{i} - \frac{Z^i}{i} \right),$$

$$g_1(X, Y, Z) = X, \quad g_2(X, Y, Z) = Y, \quad g_3(X, Y, Z) = X + Y + XY.$$

Приведем еще один пример для $n = 2$:

$$f(X, Y) = \left(\sum_{i=1}^{\infty} (-1)^{i+1} X^i / i \right) - Y,$$

$$g_1(X, Y) = \sum_{i=1}^{\infty} \frac{X^i}{i!}, \quad g_2(X, Y) = X.$$

Объясните, как можно воспользоваться результатами пункта (6) при доказательстве основных свойств элементарных p-адических степенных рядов. (Постройте соответствующие f и g_j в одной или двух конкретных ситуациях.)

§ 3. МНОГОУГОЛЬНИКИ НЬЮТОНА В СЛУЧАЕ МНОГОЧЛЕНОВ

Пусть $f(X) = 1 + \sum_{i=1}^{n} a_i X^i \in 1 + X\Omega[X]$ — многочлен степени n с коэффициентами в Ω и постоянным членом 1. Рассмотрим на вещественной координатной плоскости последовательность точек

$$(0, 0), (1, \operatorname{ord}_p a_1), (2, \operatorname{ord}_p a_2), \ldots$$
$$\ldots, (i, \operatorname{ord}_p a_i), \ldots, (n, \operatorname{ord}_p a_n).$$

(Если $a_i = 0$, то соответствующая точка пропускается либо считается лежащей «бесконечно» высоко над горизонтальной осью.) *Многоугольником Ньютона* многочлена $f(X)$ называется «выпуклая оболочка» этого множества точек, а именно самая высокая из выпуклых вниз ломаных, соединяющих точки $(0, 0)$ и $(n, \operatorname{ord}_p a_n)$ и проходящих ниже всех точек $(i, \operatorname{ord}_p a_i)$ или через них. «Механически» эта выпуклая оболочка строится

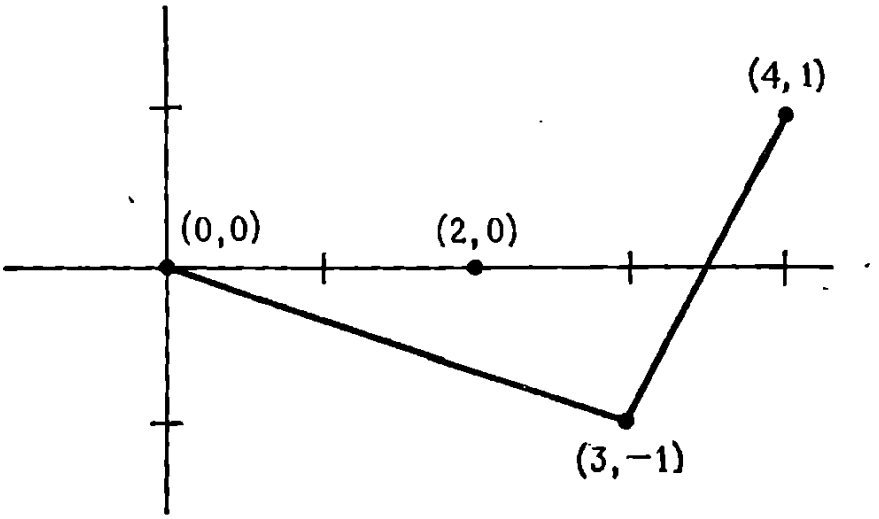


Рис. IV.1.

так. Возьмем вертикальную прямую, проходящую через точку $(0, 0)$, и начнем вращать ее вокруг $(0, 0)$ против часовой стрелки до тех пор, пока она не пройдет через одну из точек $(i, \operatorname{ord}_p a_i)$ с $i > 0$. Выберем среди таких точек последнюю[1]) $(i_1, \operatorname{ord}_p a_{i_1})$ и соединим ее отрезком с $(0, 0)$. Так находится первая сторона многоугольника Ньютона. Затем продолжим вращение этой линии вокруг точки $(i_1, \operatorname{ord}_p a_{i_1})$ до тех пор, пока она снова не пройдет через одну из последующих точек $(i, \operatorname{ord}_p a_i)$ $(i > i_1)$, выберем последнюю из этих точек $(i_2, \operatorname{ord}_p a_{i_2})$ и соединим ее отрезком с $(i_1, \operatorname{ord}_p, a_{i_1})$. Это вторая сторона искомого многоугольника. Далее продолжим вращение вокруг $(i_2, \operatorname{ord}_p a_{i_2})$ и т. д., пока не дойдем до $(n, \operatorname{ord}_p a_n)$.

На рис. 1 изображен пример многоугольника Ньютона для $f(X) = 1 + X^2 + {}^1/_3 X^3 + 3X^4$ в $\mathbb{Q}_3[X]$.

[1]) В смысле порядка индексов. — *Прим. перев.*

Вершинами многоугольника Ньютона называются точки $(i_j, \operatorname{ord}_p a_{i_j})$, в которых изменяется наклон. По определению наклон отрезка, соединяющего вершины (i, m) и (i', m'), равен отношению $(m'-m)/(i'-i)$. Под *«длиной наклона»* понимается разность $i'-i$, т. е. длина проекции соответствующей стороны многоугольника на горизонтальную ось.

Лемма 4. *В тех же обозначениях, что и выше, пусть* $f(X)=(1-X/\alpha_1)\dots(1-X/\alpha_n)$ *— разложение многочлена* $f(X)$ *на множители, где* $\alpha_i \in \Omega$ *— его корни. Положим* $\lambda_i = \operatorname{ord}_p 1/\alpha_i$. *Пусть* λ *— некоторый наклон соответствующего многоугольника Ньютона, имеющий длину* l. *Тогда среди всех чисел* λ_i *имеется в точности* l *равных* λ.

Иначе говоря, наклоны (длины наклонов) многоугольника Ньютона многочлена $f(X)$ равны p-адическим порядкам (кратностям) обратных корней для $f(X)$.

Доказательство. После подходящей нумерации корней можно считать, что $\lambda_1 \leqslant \lambda_2 \leqslant \dots \leqslant \lambda_n$. Пусть $\lambda_1 = \lambda_2 = \dots = \lambda_r < \lambda_{r+1}$. Тогда прежде всего утверждается, что первая сторона многоугольника Ньютона совпадает с отрезком, соединяющим (0, 0) и $(r, r\lambda_1)$. Как известно, каждое a_i представимо в виде умноженного на $(-1)^i$ i-го симметрического многочлена от $1/\alpha_1, 1/\alpha_2, \dots, 1/\alpha_n$, т. е. суммы всевозможных произведений по i элементов из множеств чисел $1/\alpha_i$. Так как любое такое произведение имеет p-адический порядок не меньше $i\lambda_1$, то это верно и для a_i. Значит, каждая точка $(i, \operatorname{ord}_p a_i)$ находится либо *выше* точки $(i, i\lambda_1)$, либо совпадает с ней, т. е. лежит или выше, или на прямой, соединяющей точки (0, 0) и $(r, r\lambda_1)$.

Рассмотрим теперь a_r. Существует единственное произведение из r чисел $1/\alpha_i$ с p-адическим порядком $r\lambda_1$, а именно $1/(\alpha_1 \alpha_2 \dots \alpha_r)$. Все остальные произведения из r элементов имеют p-адический порядок $> r\lambda_1$, так как в эти произведения входит по крайней мере один из элементов $\lambda_{r+1}, \lambda_{r+2}, \dots, \lambda_n$. Таким образом, a_r равно сумме числа с порядком $r\lambda_1$ и чисел с порядком $> r\lambda_1$. Поэтому $\operatorname{ord}_p a_r = r\lambda_1$ по «принципу равнобедренного треугольника».

Пусть теперь $i > r$. Как и выше, мы устанавливаем, что все произведения по i чисел из $1/\alpha_i$ имеют порядок $> i\lambda_1$. Следовательно, $\operatorname{ord}_p a_i > i\lambda_1$. Если вспомнить теперь, как строится многоугольник Ньютона, то сразу станет ясно, что его первая сторона совпадает с отрезком, соединяющим точки $(0, 0)$ и $(r, r\lambda_1)$.

Если $\lambda_s < \lambda_{s+1} = \lambda_{s+2} = \ldots = \lambda_{s+r} < \lambda_{s+r+1}$, то совпадение отрезка, соединяющего $(s, \lambda_1 + \lambda_2 + \ldots + \lambda_s)$ и $(s+r, \lambda_1 + \lambda_2 + \ldots + \lambda_s + r\lambda_{s+1})$, с одной из сторон многоугольника Ньютона, доказывается точно так же, и мы оставляем доказательство читателю. □

§ 4. МНОГОУГОЛЬНИКИ НЬЮТОНА В СЛУЧАЕ СТЕПЕННЫХ РЯДОВ

Пусть теперь $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\Omega[[X]]$ — некоторый степенной ряд[1]). Многочлен $f_n(X) = 1 + \sum_{i=1}^{n} a_i X^i \in 1 + X\Omega[X]$ называется n-й частичной суммой ряда $f(X)$. Многоугольник Ньютона для $f(X)$ определяется как «предел» многоугольников Ньютона для $f_n(X)$. Точнее, этот многоугольник строится по тому же рецепту, что и в случае многочленов: наносим на плоскость точки $(0, 0)$, $(1, \operatorname{ord}_p a_1), \ldots, (i, \operatorname{ord}_p a_i), \ldots$; вращаем вертикальную прямую вокруг $(0, 0)$, пока она не пройдет через некоторую точку $(i, \operatorname{ord}_p a_i)$, затем продолжаем вращение вокруг последней из этих точек и т. д. При этом возможны следующие три случая[2]).

(1) Получается многоугольник с бесконечным числом сторон конечной длины. Таков, например, многоугольник Ньютона ряда $f(X) = 1 + \sum_{i=1}^{\infty} p^{i^2} X^i$; он представ-

---

[1]) В этом параграфе ряды предполагаются отличными от многочленов, т. е. имеющими бесконечно много неиулевых коэффициентов. — *Прим. перев.*

[2]) Ниже всегда предполагается, что f имеет нетривиальный ($\neq \{0\}$) диск сходимости. — *Прим. перев.*

ляет собой ломаную, вписанную в правую половину параболы $y = x^2$ (рис. 2).

(2) Вращаемая прямая попадает в такое положение, при котором на ней оказывается сразу бесконечно много точек $(i, \operatorname{ord}_p a_i)$. В этом случае многоугольник Ньютона имеет конечное число сторон конечной длины и одну, а именно последнюю, — бесконечной длины. Например, многоугольник Ньютона ряда $f(X) = 1 + \sum_{i=1}^{\infty} X^i$ состоит из одного бесконечно длинного горизонтального луча из точки (0, 0).

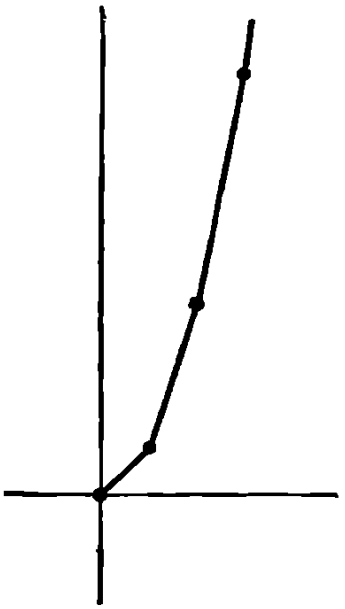


Рис. IV.2.

(3) Сама прямая, вращаемая вокруг некоторой точки, в какой-то момент еще не содержит ни одной из последующих точек $(i, \operatorname{ord}_p a_i)$, но при сколь угодно малом дальнейшем повороте она уже пройдет над некоторой из этих точек $(i, \operatorname{ord}_p a_i)$. Один из простейших примеров такого сорта дает ряд $f(X) = 1 + \sum_{i=1}^{\infty} pX^i$. В этом случае вертикаль, проходящую через (0, 0), можно повернуть до горизонтального положения, но при любом дальнейшем вращении она пройдет над некоторыми точками $(i, 1)$. В подобных ситуациях в качестве последнего наклона многоугольника Ньютона берется точная верхняя грань всех наклонов, для которых соответствующая прямая проходит ниже всех последующих $(i, \operatorname{ord}_p a_i)$. В рассмотренном примере этот наклон равен 0 и многоугольник Ньютона состоит из одного горизонтального луча (рис. 3).

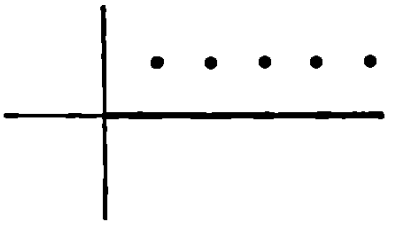


Рис. IV.3.

Многоугольник Ньютона в случае многочленов позволяет быстро определить, на каких радиусах расположены обратные корни. Ниже будет показано, что аналогично по многоугольнику Ньютона степенного ряда $f(X)$ можно судить о расположении нулей $f(X)$. Но вначале рассмотрим один особенно яркий пример.

Пусть

$$f(X)=1+\frac{X}{2}+\frac{X^2}{3}+\ldots+\frac{X^i}{i+1}+\ldots=-\frac{1}{X}\log_p(1-X).$$

Многоугольник Ньютона для $f(X)$ (см. рис. 4 в случае $p=3$) — это ломаная, последовательно соединяющая вершины $(0,\ 0)$, $(p-1,\ -1)$, $(p^2-1,\ -2)$, ..., $(p^j-1,\ -j)$, ... (На нем реализуется возможность (1)

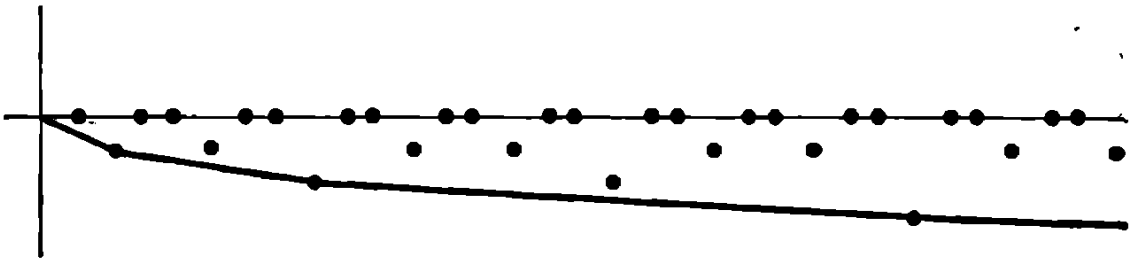


Рис. IV.4.

из приведенного выше списка.) Предположим, что для степенных рядов верен аналог леммы 4 из § 3. Тогда по виду этого многоугольника Ньютона следовало бы ожидать, что $f(X)$ имеет ровно $p^{j+1}-p^j$ нулей с p-адическим порядком $1/(p^{j+1}-p^j)$.

Но посмотрим, каковы же в действительности нули $-\log_p(1-X)/X$? Прежде всего, если $x=1-\zeta$, где ζ — примитивный корень из 1 степени p^{j+1}, то, как мы знаем из упр. 7 к § III. 4, $\mathrm{ord}_p x=1/(p^{j+1}-p^j)$. Отсюда $\log_p(1-x)=\log_p\zeta=0$ (см. обсуждение $\log_p$ в § 1). Тем самым найдены все предсказанные нули, так как существует $p^{j+1}-p^j$ примитивных корней степени p^{j+1} из 1. Имеет ли $f(X)$ нули еще где-нибудь на $D(1^-)$?

Пусть $x\in D(1^-)$ — один из таких нулей. Тогда для любого j точка $x_j=1-(1-x)^{p^j}\in D(1^-)$ также будет нулем, поскольку $\log_p(1-x_j)=p^j\log_p(1-x)=0$. Но при достаточно большом j справедливо включение $x_j\in$ $\in D(p^{-1/(p-1)-})$, откуда $1-x_j=\exp_p(\log_p(1-x_j))=$

$= \exp_p 0 = 1$. Следовательно, $(1-x)^{p^j} = 1$ и x совпадает с одним из рассмотренных выше нулей. Таким образом, форма многоугольника Ньютона полностью соответствует нашей информации о нулях ряда $\log_p(1-X)$.

Перейдем теперь к доказательству того, что многоугольник Ньютона играет для степенных рядов такую же роль, как и для многочленов. Но вначале установим один гораздо более простой результат, согласно которому по виду многоугольника Ньютона можно сразу узнать радиус сходимости соответствующего степенного ряда.

Лемма 5. *Пусть b — точная верхняя грань множества всех наклонов многоугольника Ньютона ряда $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\,\Omega[[X]]$. Тогда его радиус сходи-*

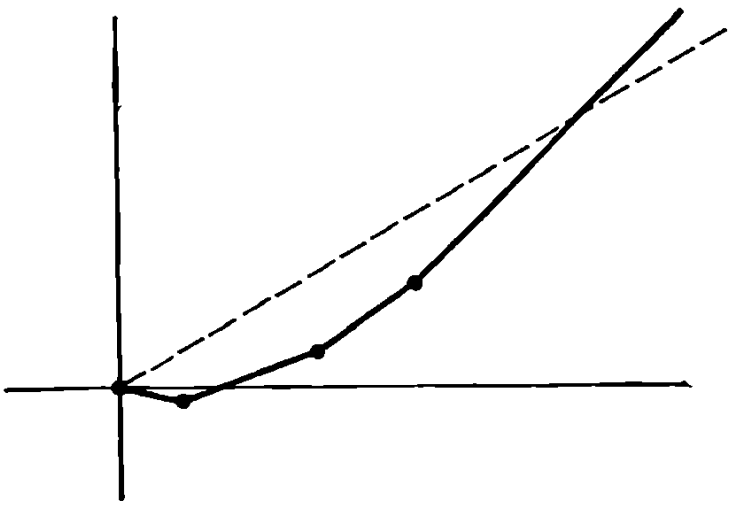


Рис. IV.5.

мости равен p^b (b может быть бесконечным, и в этом случае $f(X)$ сходится на всем Ω).

Доказательство. Пусть вначале $|x|_p < p^b$, т. е. $\operatorname{ord}_p x > -b$. Положим $\operatorname{ord}_p x = -b'$. Тогда $b' < b$ и $\operatorname{ord}_p(a_i x^i) = \operatorname{ord}_p a_i - ib'$. Но, очевидно (см. рис. 5), для достаточно больших i точка $(i, \operatorname{ord}_p a_i)$ лежит сколь угодно выше точки $(i, b'i)$. Иначе говоря, $\operatorname{ord}_p(a_i x^i) \to \infty$ и $f(X)$ сходится для таких $X = x$.

Пусть теперь $|x|_p > p^b$, т. е. $\operatorname{ord}_p x = -b' < -b$. Тогда по тем же соображениям имеется бесконечно

много значений i, для которых $\operatorname{ord}_p(a_i x^i) = \operatorname{ord}_p a_i - b'i$ отрицательно. Поэтому $f(x)$ не сходится. Отсюда мы заключаем, что радиус сходимости ряда $f(X)$ равен в точности p^b. □

Замечание. Эта лемма ничего не утверждает о сходимости или расходимости в точках, где $|x|_p = p^b$. Легко понять, что сходимость для таких x (т. е. «на граничной окружности») возможна лишь тогда, когда реализуется третий из перечисленных выше случаев, причем сходимость имеет место тогда и только тогда, когда расстояние по вертикали от $(i, \operatorname{ord}_p a_i)$ до последней (бесконечной) стороны стремится к ∞ при $i \to \infty$. Пример такого поведения дает ряд $f(X) = 1 + \sum_{i=1}^{\infty} p^i X^{p^i}$, многоугольник Ньютона которого совпадает с горизонтальным лучом из точки (0, 0). Этот ряд сходится, если $\operatorname{ord}_p x = 0$.

Прежде чем приступить к доказательству аналога леммы 4 для степенных рядов, сделаем одно заключительное замечание. Пусть $c \in \Omega$, $\operatorname{ord}_p c = \lambda$ и $g(X) = f(X/c)$. Тогда многоугольник Ньютона для g получается из соответствующего многоугольника для f поточечным вычитанием графика линейной функции $y = \lambda x$, т. е. прямой, проходящей через точку (0, 0) с наклоном λ. Действительно, если $f(X) = 1 + \sum a_i X^i$, а $g(X) = 1 + \sum b_i X^i$, то $\operatorname{ord}_p b_i = \operatorname{ord}_p (a_i/c^i) = \operatorname{ord}_p a_i - \lambda i$.

Лемма 6. *Предположим, что λ_1 — первый наклон многоугольника Ньютона ряда $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\,\Omega[[X]]$. Пусть $c \in \Omega$, $\operatorname{ord}_p c = \lambda \leqslant \lambda_1$. Предположим также, что $f(X)$ сходится на замкнутом диске $D(p^\lambda)$ (по лемме 5 это выполнено автоматически, если $\lambda < \lambda_1$ или многоугольник Ньютона для $f(X)$ имеет более одной стороны). Пусть*

$$g(X) = (1 - cX) f(X) \in 1 + X\,\Omega[[X]].$$

Тогда многоугольник Ньютона для $g(X)$ получается добавлением к отрезку, соединяющему точки (0, 0) *и*

(1, λ), *многоугольника Ньютона для* $f(X)$, *сдвинутого на* 1 *по горизонтали и на* λ *по вертикали. Иначе говоря, многоугольник Ньютона ряда* $g(X)$ *получается «присоединением» многоугольника Ньютона степенного ряда* $f(X)$ *к многоугольнику Ньютона многочлена* $(1-cX)$. *Кроме того, если* $f(X)$ *имеет последний наклон* λ_f *и сходится на* $D(p^{\lambda_f})$, *то* g *также сходится на* $D(p^{\lambda_f})$.

Доказательство. Прежде всего сведем доказательство к разбору специального случая $c=1$, $\lambda=0$. Предположим, что для этого случая лемма уже установлена и мы имеем $f(X)$ и $g(X)$, удовлетворяющие условиям. Тогда для $f_1(X)=f(X/G)$ и $g_1(X)=(1-X)f_1(X)$ выполнены все те же условия, но с 1, 0, $\lambda_1-\lambda$ вместо c, λ, λ_1 (см. замечание, непосредственно предшествующее формулировке леммы). По предположению, для f_1 и g_1 лемма верна, откуда мы находим форму многоугольника Ньютона для $g_1(X)$ (и устанавливаем сходимость g_1 на $D(p^{\lambda_f-\lambda})$, если f сходится на $D(p^{\lambda_f})$). Так как $g(X)=g_1(cX)$, то можно еще раз воспользоваться упомянутым замечанием, получить требуемое утверждение о многоугольнике Ньютона для $g(X)$ (см. рис. 6).

Итак, лемму 6 достаточно доказать при $c=1$, $\lambda=0$. Пусть $g(X)=1+\sum_{i=1}^{\infty} b_i X^i$. Тогда в силу равенства $g(X)=(1-X)f(X)$ имеем $b_{i+1}=a_{i+1}-a_i$ для $i\geqslant 0$ $(a_0=1)$. Поэтому

$$\operatorname{ord}_p b_{i+1}\geqslant \min(\operatorname{ord}_p a_{i+1},\ \operatorname{ord}_p a_i),$$

причем имеет место равенство, если $\operatorname{ord}_p a_{i+1}\neq \operatorname{ord}_p a_i$ (по принципу равнобедренного треугольника). Так как обе точки $(i,\ \operatorname{ord}_p a_i)$ и $(i,\ \operatorname{ord}_p a_{i+1})$ лежат на или над стороной многоугольника Ньютона для $f(X)$, то же самое справедливо и для $(i,\ \operatorname{ord}_p b_{i+1})$. Если $(i,\ \operatorname{ord}_p a_i)$ — вершина, то $\operatorname{ord}_p a_{i+1}>\operatorname{ord}_p a_i$, а потому $\operatorname{ord}_p b_{i+1}=\operatorname{ord}_p a_i$. Отсюда следует, что многоугольник Ньютона имеет требуемый вид вплоть до своей последней вершины. Таким образом, остается разобрать случай, когда многоугольник Ньютона для $f(X)$ содержит последнюю бесконечно длинную сторону наклона λ_f, и показать, что в этом случае то же самое верно для $g(X)$; более

того, если $f(X)$ сходится на $D(p^{\lambda_f})$, то $g(X)$ сходится там же. В силу неравенства $\operatorname{ord}_p b_{i+1} \geqslant \min(\operatorname{ord}_p a_{i+1}, \operatorname{ord}_p a_i)$ из сходимости $f(X)$ немедленно следует сходимость $g(X)$ в той же области. Итак, необходимо исключить возможность, что многоугольник Ньютона ряда $g(X)$ имеет

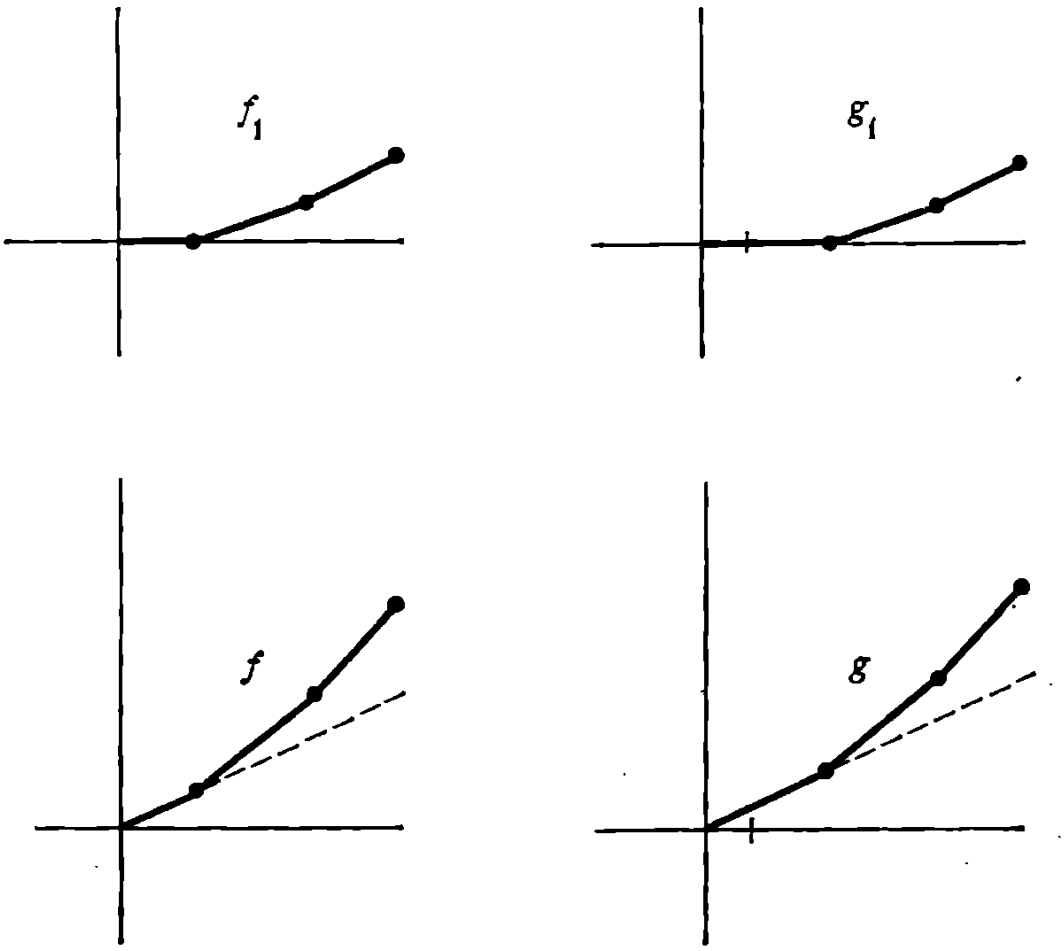


Рис. IV.6.

больший наклон λ_g, чем λ_f. Если бы это выполнялось, то при некотором достаточно большом i точка $(i+1, \operatorname{ord}_p a_i)$ лежала бы ниже соответствующей точки многоугольника Ньютона для $g(X)$. Поэтому мы имели бы $\operatorname{ord}_p b_j > \operatorname{ord}_p a_i$ для всех $j \geqslant i+1$. Из этого, во-первых, следует равенство $\operatorname{ord}_p a_{i+1} = \operatorname{ord}_p a_i$, потому что $a_{i+1} = b_{i+1} + a_i$; затем по тем же соображениям $\operatorname{ord}_p a_{i+2} = \operatorname{ord}_p a_{i+1}$ и т. д., $\operatorname{ord}_p a_j = \operatorname{ord}_p a_i$ для всех $j > i$. Но это противоречит предполагаемой сходимости $f(X)$ на $D(1)$. □

Лемма 7. *Пусть* λ_1 *— первый наклон многоугольника Ньютона ряда* $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\Omega[[X]]$. *Предположим, что* $f(X)$ *сходится на замкнутом диске* $D(p^{\lambda_1})$, *а, кроме того, линия, проходящая через* (0, 0) *с наклоном* λ_1, *содержит некоторую точку* $(i, \operatorname{ord}_p a_i)$. *(Оба эти условия автоматически выполнены, если многоугольник Ньютона имеет более одного наклона.) Тогда существует число* $x \in \Omega$, *для которого* $\operatorname{ord}_p x = -\lambda_1$, *а* $f(x) = 0$.

Доказательство. Для простоты рассмотрим вначале случай $\lambda_1 = 0$, а затем сведем доказательство леммы к этому случаю. Итак, пусть $\lambda_1 = 0$. Тогда $\operatorname{ord}_p a_i \geqslant 0$ для всех i и $\operatorname{ord}_p a_i \to \infty$ при $i \to \infty$. Пусть $N \geqslant 1$ равно наибольшему i, для которого $\operatorname{ord}_p a_i = 0$. (Очевидно, N есть длина первой стороны многоугольника Ньютона ряда $f(X)$, за исключением случая, когда этот многоугольник совпадает с горизонтальным лучом.) Пусть $f_n(X) = 1 + \sum_{i=1}^{n} a_i X^i$. По лемме 4 многочлен $f_n(X)$ при $n \geqslant N$ имеет в точности N корней $x_{n,1}, \ldots, x_{n,N}$ с $\operatorname{ord}_p x_{n,i} = 0$. Пусть $x_N = x_{N,1}$, а x_{n+1} при $n \geqslant N$ — любой из элементов $x_{n+1,1}, \ldots, x_{n+1,N}$ с минимальной нормой разности $|x_{n+1,i} - x_n|_p$. Утверждается, что $\{x_n\}$ — последовательность Коши и ее предел x обладает нужными свойствами.

Для $n \geqslant N$ обозначим через S_n множество корней многочлена $f_n(X)$ (с учетом их кратностей). Тогда при $n \geqslant N$ имеем

$$|f_{n+1}(x_n) - f_n(x_n)|_p = |f_{n+1}(x_n)|_p =$$

(так как $f_n(x_n) = 0$)

$$= \prod_{x \in S_{n+1}} \left|1 - \frac{x_n}{x}\right|_p = \prod_{i=1}^{N} \left|1 - \frac{x_n}{x_{n+1,i}}\right|_p =$$

(так как $|1 - x_n/x|_p = 1$, если $x \in S_{n+1}$ и $\operatorname{ord}_p x < 0$)

$$= \prod_{i=1}^{N} |x_{n+1,i} - x_n|_p \geqslant$$

(так как $|x_{n+1,i}|_p = 1$)

$$\geqslant |x_{n+1} - x_n|_p^N$$

в силу выбора x_{n+1}. Поэтому

$$|x_{n+1} - x_n|_p^N \leqslant |f_{n+1}(x_n) - f_n(x_n)|_p = |a_{n+1}x_n^{n+1}|_p = |a_{n+1}|_p.$$

Поскольку $|a_{n+1}|_p \to 0$ при $n \to \infty$, $\{x_n\}$ является последовательностью Коши. Пусть $x_n \to x \in \Omega$. Тогда $f(x) = \lim\limits_{n\to\infty} f_n(x)$. Но

$$|f_n(x)|_p = |f_n(x) - f_n(x_n)|_p =$$

$$= |x - x_n|_p \left| \sum_{i=1}^{n} a_i \frac{x^i - x_n^i}{x - x_n} \right|_p \leqslant |x - x_n|_p,$$

потому что $|a_i|_p \leqslant 1$ и $\left|(x^i - x_n^i)/(x - x_n)\right|_p = |x^{i-1} + x^{i-2}x_n + x^{i-3}x_n^2 + \ldots + x_n^{i-1}|_p \leqslant 1$. Следовательно, $f(x) = \lim\limits_{n\to\infty} f_n(x) = 0$. Это доказывает лемму при $\lambda_1 = 0$. Теперь легко вывести общий случай. Пусть $\pi \in \Omega$ — произвольное число с $\operatorname{ord}_p \pi = \lambda_1$. Заметим, что такое π существует: можно взять, например, корень степени i из a_i, для которого $(i, \operatorname{ord}_p a_i)$ лежит на прямой с наклоном λ_1, проходящей через $(0, 0)$. Пусть теперь $g(X) = f(X/\pi)$. Тогда $g(X)$ удовлетворяет условиям леммы с $\lambda_1 = 0$. Таким образом, по только что доказанному существует x_0 с $\operatorname{ord}_p x_0 = 0$, и $g(x_0) = 0$. Пусть $x = x_0/\pi$. Тогда $\operatorname{ord}_p x = -\lambda_1$ и $f(x) = f(x_0/\pi) = g(x_0) = 0$. □

Лемма 8. *Пусть ряд* $f(X) = 1 + \sum\limits_{i=1}^{\infty} a_i X^i \in 1 + X\Omega[[X]]$ *сходится к нулю при некотором* α. *Тогда ряд* $g(X) = 1 + \sum\limits_{i=1}^{\infty} b_i X^i$, *полученный делением ряда* $f(X)$ *на* $(1 - X/\alpha)$, *или, что то же самое, умножением на ряд* $1 + X/\alpha + X^2/\alpha^2 + \ldots + X^i/\alpha^i + \ldots$, *сходится на* $D(|\alpha|_p)$.

Доказательство. Пусть $f_n(X) = 1 + \sum\limits_{i=1}^{n} a_i X^i$. Очевидно,

$$b_i = 1/\alpha^i + a_1/\alpha^{i-1} + a_2/\alpha^{i-2} + \ldots + a_{i-1}/\alpha + a_i,$$

откуда

$$b_i\alpha^i = f_i(\alpha).$$

Следовательно, $|b_i\alpha^i|_p = |f_i(\alpha)|_p \to 0$ при $i \to \infty$, потому что $f(\alpha) = 0$. □

Теорема 14 (p-адическая подготовительная теорема Вейерштрасса). *Предположим, что ряд* $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\Omega[[X]]$ *сходится на* $D(p^\lambda)$. *Пусть* N *— общая длина, если она конечна (т. е. если многоугольник Ньютона ряда* $f(X)$ *не имеет последней бесконечнодлинной стороны наклона* λ*), проекции на горизонтальную ось всех сторон с наклоном* $\leqslant \lambda$. *Если же многоугольник Ньютона для* $f(X)$ *имеет последний наклон* λ, *то положим* N *равным наибольшему* i, *для которого* $(i, \operatorname{ord}_p a_i)$ *лежит на последней стороне (существование такого* i *следует из сходимости* $f(X)$ *на* $D(p^\lambda)$). *Тогда найдутся такой многочлен* $h(X) \in 1 + X\Omega[X]$ *степени* N *и такой степенной ряд* $g(X) = 1 + \sum_{i=1}^{\infty} b_i X^i$, *сходящийся и не обращающийся в нуль на* $D(p^\lambda)$, *что*

$$h(X) = f(X) \cdot g(X).$$

Многочлен $h(X)$ *определен однозначно этими свойствами, а его многоугольник Ньютона совпадает с многоугольником Ньютона ряда* $f(X)$ *вплоть до точки* $(N, \operatorname{ord}_p a_N)$.

Доказательство. Применим индукцию по N. Пусть вначале $N = 0$. Тогда нужно установить существование ряда $g(X)$, обратного к $f(X)$, его сходимость и необращение в нуль на $D(p^\lambda)$. Это утверждение было частью упр. 3 к § 2, но в силу его важности мы приведем здесь его доказательство для тех, кто пропустил это упражнение. Как обычно (см. доказательства лемм 6 и 7, а также замечание, предшествующее формулировке леммы 6), доказательство можно свести к случаю $\lambda = 0$.

Итак, пусть $f(X) = 1 + \sum a_i X^i$, $\operatorname{ord}_p a_i > 0$, $\operatorname{ord}_p a_i \to \infty$, $g(X) = 1 + \sum b_i X^i$. Из соотношения $f(X)\,g(X) = 1$ получается рекуррентная формула

$$b_i = -(b_{i-1}a_1 + b_{i-2}a_2 + \ldots + b_1 a_{i-1} + a_i), \quad i \geqslant 1,$$

из которой индукцией по i легко вывести неравенства $\operatorname{ord}_p b_i > 0$. Поэтому осталось показать, что $\operatorname{ord}_p b_i \to \infty$ при $i \to \infty$. Возьмем достаточно большое M. Выберем затем такое m, что $\operatorname{ord}_p a_i > M$ при $i > m$. Пусть

$$\varepsilon = \min(\operatorname{ord}_p a_1, \operatorname{ord}_p a_2, \ldots, \operatorname{ord}_p a_m) > 0.$$

Тогда утверждается, что $\operatorname{ord}_p b_i > \min(M, n\varepsilon)$ при $i > nm$. Отсюда, конечно, получается требуемое соотношение $\operatorname{ord}_p b_i \to \infty$. Утверждение докажем индукцией по n. Для $n = 0$ оно очевидно. Предположим, что $n \geqslant 1$, $i > nm$. По рекуррентной формуле

$$b_i = -(b_{i-1}a_1 + \ldots + b_{i-m}a_m + b_{i-(m+1)}a_{m+1} + \ldots + a_i).$$

Для членов $b_{i-j}a_j$ с $j > m$ имеет место неравенство $\operatorname{ord}_p(b_{i-j}a_j) \geqslant \operatorname{ord}_p a_j > M$, в то время как $\operatorname{ord}_p(b_{i-j}a_j) \geqslant \geqslant \operatorname{ord}_p b_{i-j} + \varepsilon > \min(M, (n-1)\varepsilon) + \varepsilon$ при $j \leqslant m$ по индуктивному предположению (так как $i - j > (n-1)m$) и по определению ε. Поэтому все слагаемые в формуле для b_i имеют $\operatorname{ord}_p > \min(M, n\varepsilon)$. Это доказывает утверждение, а следовательно, и теорему при $N = 0$.

Предположим теперь, что $N \geqslant 1$ и теорема уже доказана для $N - 1$. Пусть $\lambda_1 \leqslant \lambda$ — первый наклон многоугольника Ньютона ряда $f(X)$. Применяя лемму 7, найдем α, для которого $f(\alpha) = 0$ и $\operatorname{ord}_p \alpha = -\lambda_1$. Положим

$$f_1(X) = f(X)\left(1 + \frac{X}{\alpha} + \frac{X^2}{\alpha^2} + \ldots + \frac{X^i}{\alpha^i} + \ldots\right) =$$
$$= 1 + \sum a_i' X^i \in 1 + X\Omega[[X]].$$

По лемме 8 ряд $f_1(X)$ сходится на $D(p^{\lambda_1})$. Пусть $c = 1/\alpha$, так что $f(X) = (1 - cX) f_1(X)$. Если бы первый наклон λ_1' многоугольника Ньютона для $f_1(X)$ был меньше λ_1, то по лемме 7 ряд $f_1(X)$ обладал бы корнем с p-адическим порядком $-\lambda_1'$, а тогда то же самое выполнялось бы и для $f(X)$, но, как легко проверить, это невозможно. Следовательно, $\lambda_1' \geqslant \lambda_1$ и мы находимся в условиях леммы 6 (с f_1, f, λ_1' и λ_1 вместо f, g, λ_1 и λ соответственно). Тогда по этой лемме $f_1(X)$ имеет тот же многоугольник Ньютона, что и $f(X)$, если только исключить у последнего сторону, соединяющую (0, 0) и (1, λ_1). В частности, f и f_1 имеют одинаковые радиусы сходимости. Кроме того, даже в том случае, когда λ

совпадает с последним наклоном многоугольника Ньютона ряда f (а поэтому и f_1), ряд f_1 сходится на $D(p^\lambda)$, поскольку f сходится на $D(p^\lambda)$ по предположению [1]).

Итак, $f_1(X)$ удовлетворяет требованиям теоремы с $N-1$ вместо N. По индуктивному предположению можно найти такой многочлен $h_1(X) \in 1+X\Omega[X]$ степени $N-1$ и такой ряд $g(X) \in 1+X\Omega[[X]]$, сходящийся и не обращающийся в нуль на $D(p^\lambda)$, что

$$h_1(X) = f_1(X) \cdot g(X).$$

Умножим обе части последнего равенства на $(1-cX)$ и положим $h(X) = (1-cX)\,h_1(X)$. Тогда

$$h(X) = f(X) \cdot g(X)$$

и $h(X)$ и $g(X)$ обладают нужными свойствами.

Наконец, так как f имеет в точности N нулей в $D(p^\lambda)$, из этого немедленно следует, что $h(X)$ единствен. Действительно, этот многочлен имеет степень N, постоянный член 1 и все N нулей ряда $f(X)$ являются также его нулями [2]). □

Следствие. *Если сторона многоугольника Ньютона ряда* $f(X) \in 1+X\Omega[[X]]$ *имеет конечную длину* N *и наклон* λ, *то существует в точности* N *значений* x [3]), *для которых* $f(x)=0$ *и* $\operatorname{ord}_p x = -\lambda$.

В качестве другого следствия теоремы 14 можно установить, что любой всюду сходящийся степенной ряд разлагается в бесконечное произведение линейных множителей $(1-X/r)$ по всем своим нулям r. В частности, всюду сходящийся и нигде не обращающийся в нуль ряд должен быть постоянным (см. ниже упр. 13). В отличие от этого в вещественном и комплексном случае существуют непостоянные ряды без нулей, напри-

---

[1]) Это утверждение, обратное к сформулированному в конце леммы 6, доказывается по существу тем же методом. — *Прим. перев.*

[2]) Это рассуждение проходит, если все корни различны. Аккуратное доказательство требует индукции. — *Прим. перев.*

[3]) С учетом кратностей, которые позволяет определить предыдущая теорема. — *Прим. перев.*

мер ряд функции e^x (или более общий ряд $e^{h(x)}$, где h — любой всюду сходящийся степенной ряд). В комплексном анализе разложение в бесконечное произведение всюду сходящегося степенного ряда по его нулям сложнее, чем в p-адическом случае; при этом для получения «произведения Вейерштрасса» «целой» функции комплексного переменного необходимо вводить дополнительные экспоненциальные множители.

Таким образом, простой вид разложения в бесконечное произведение в p-адическом случае, существование которого следует из теоремы 14, возможен благодаря отсутствию всюду сходящихся экспоненциальных функций. Значит, тут нам с плохой сходимостью $\exp_p$ крупно повезло. Но в других обстоятельствах, скажем в теории p-адических дифференциальных уравнений, отсутствие хорошо сходящейся экспоненты очень усложняет жизнь.

Упражнения

1. Найдите многоугольник Ньютона для следующих многочленов:

(i) $1-X+pX^2$; (ii) $1-X^3/p^2$; (iii) $1+X^2+pX^4+p^3X^6$;

(iv) $\sum_{i=1}^{p} iX^{i-1}$; (v) $(1-X)(1-pX)(1-p^3X)$ (двумя способами);

(vi) $\prod_{i=1}^{p^2}(1-iX)$.

2. (a) Пусть $f(X) \in 1+X\mathbb{Z}_p[X]$ — многочлен, многоугольник Ньютона которого состоит из одного отрезка, соединяющего точки $(0, 0)$ и (n, m). Покажите, что $f(X)$ неразложим в произведение двух многочленов положительной степени с коэффициентами в $\mathbb{Z}_p$, если n и m взаимно просты.

(b) Используя пункт (a), дайте другое доказательство критерия неприводимости Эйзенштейна (см. упр. 13 к § I.5).

(c) Верно ли обратное к (a), т. е. всякий ли неприводимый многочлен имеет многоугольник Ньютона указанного типа (докажите или постройте контрпример)?

3. Пусть $f(X) \in 1+X\mathbb{Z}_p[X]$ — многочлен степени $2n$. Пусть нам известно, что для всякого обратного корня α многочлена $f(X)$ обратным корнем является также p/α (с той же кратностью). Что можно сказать о форме многоугольника Ньютона в этом случае?

Нарисуйте все возможные виды многоугольников Ньютона для таких $f(X)$ при $n=1, 2, 3, 4$.

4. Найдите многоугольники Ньютона следующих степенных рядов:

(i) $\sum_{i=0}^{\infty} X^{p^i-1}/p^i$; (ii) $\sum_{i=0}^{\infty} ((pX)^i + X^{p^i})$;

(iii) $\sum_{i=0}^{\infty} i! X^i$; (iv) $\sum_{i=0}^{\infty} X^i/i!$;

(v) $(1-pX^2)/(1-p^2X^2)$; (vi) $(1-p^2X)/(1-pX)$;

(vii) $\prod_{i=0}^{\infty} (1-p^iX)$; (viii) $\sum_{i=0}^{\infty} p^{[i\sqrt{2}]}X^i$.

5. Покажите, что все наклоны сторон конечной длины многоугольника Ньютона для степенного ряда являются рациональными числами, но что наклон последней бесконечной стороны (если она существует) не обязательно таков (постройте пример).

6. Покажите, построив контрпример, что лемма 7 не верна, если опустить условие существования точки $(i, \operatorname{ord}_p a_i)$ с $i>0$ на прямой, проходящей через (0, 0) с наклоном λ_1.

7. Покажите, построив контрпример, что лемма 6 не верна, если опустить условие сходимости $f(X)$ на $D(p^\lambda)$.

8. Пусть $f(X)=1+\sum_{i=1}^{\infty} a_iX^i \in 1+X\Omega[[X]]$ — ряд, сходящийся на $D(p^\lambda)$. Докажите, что $\max_{x\in D(p^\lambda)} |f(x)|_p$ достигается на множестве точек x с $|x|_p=p^\lambda$, т. е. на «граничной окружности», и что p-адический порядок этого максимума равен

$$\min_{i=0,\ 1,\ \ldots} (\operatorname{ord}_p a_i - i\lambda),$$

т. е. минимальному «расстоянию» по вертикали (которое может быть отрицательным) от прямой, проходящей через (0, 0) с наклоном λ, до точки $(i, \operatorname{ord}_p a_i)$.

9. Пусть $f(X)=\sum_{i=0}^{\infty} a_iX^i \in \mathbb{Z}_p[[X]]$. Предположим, что $f(X)$ сходится в *замкнутом* единичном диске $D(1)$. Кроме того, предположим, что по крайней мере два коэффициента a_i не делятся на p. Докажите, что $f(X)$ имеет нуль на $D(1)$.

10. Пусть $f(X)$ — степенной ряд сходящийся и имеющий бесконечно много нулей на $D(r)$. Покажите, что тогда $f(X)$ тождественно равен нулю.

11. Докажите, что $E_p(X)$ сходится только на $D(1^-)$ (т. е. не на всем $D(1)$). (*Указание*: воспользуйтесь упр. 9 и 10 и покажите, что если E_p имеет хотя бы один нуль, то их бесконечно много.)

12. Пусть $g(X)=h(X)/f(X)$, где $g(X)\in 1+X\Omega[[X]]$ и все коэффициенты этого ряда лежат в $D(1)$, а $h(X)$ и $f(X)\in 1+X\Omega[X]$ — два многочлена, не имеющие общих корней. Докажите, что все коэффициенты $h(X)$ и $f(X)$ также лежат в $D(1)$.

13. Пусть $f(X)\in 1+X\Omega[[X]]$ сходится всюду на Ω. Для любого вещественного λ обозначим через $h_\lambda(X)$ многочлен $h(X)$ из теоремы 14. Докажите, что $h_\lambda\to f$ при $\lambda\to\infty$ (т. е. каждый коэффициент многочлена h_λ стремится к соответствующему коэффициенту ряда f). Докажите, что если f не миогочлен, то он имеет бесконечное число нулей (но не более чем счетное: $r_1, r_2, \ldots$) и $f(X)=\prod_{i=1}^{\infty}(1-X/r_i)$. В частности, не существует всюду сходящихся и нигде не обращающихся в нуль степенных рядов, кроме констант (в противоположность комплексному и вещественному случаям, где степенной ряд $e^{h(X)}$ всюду сходится и не имеет нулей для любого всюду сходящегося степенного ряда $h(X)$).

Глава V

РАЦИОНАЛЬНОСТЬ ДЗЕТА-ФУНКЦИИ СИСТЕМЫ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ НАД КОНЕЧНЫМ ПОЛЕМ

§ 1. ГИПЕРПОВЕРХНОСТИ И ИХ ДЗЕТА-ФУНКЦИИ

Пусть F — некоторое поле. Через $\mathbb{A}_F^n$ обозначим *n-мерное аффинное пространство над* F, т. е. множество упорядоченных наборов $(x_1, \ldots, x_n)$ по n элементов x_i из F. Пусть $f(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$ — некоторый многочлен от n переменных $X_1, \ldots, X_n$. Под *аффинной гиперповерхностью*, заданной уравнением $f=0$, понимается множество

$$H_f \overset{\text{def}}{=} \{(x_1, \ldots, x_n) \in \mathbb{A}_F^n \mid \quad f(x_1, \ldots, x_n) = 0\}.$$

Число $n-1$ называется *размерностью* гиперповерхности H_f. Если H_f одномерна, т. е. $n=2$, она называется *аффинной кривой*.

Сопутствующим к понятию аффинного пространства является *проективное пространство*. Проективное пространство над F размерности n обозначается $\mathbb{P}_F^n$ и определяется как множество классов эквивалентности элементов из $\mathbb{A}_F^{n+1} - \{(0, 0, \ldots, 0)\}$ по отношению эквивалентности $(x_0, x_1, \ldots, x_n) \sim (x_0', x_1', \ldots, x_n') \Leftrightarrow \exists \lambda \in F^\times$, для которого $x_i' = \lambda x_i$, $i = 0, \ldots, n$. Иначе говоря, множество $\mathbb{P}_F^n$ есть множество всех прямых в $\mathbb{A}_F^{n+1}$, проходящих через начало координат.

Пространство $\mathbb{A}_F^n$ можно вложить в $\mathbb{P}_F^n$ при помощи отображения $(x_1, \ldots, x_n) \longmapsto (1, x_1, \ldots, x_n)$. Образ $\mathbb{A}_F^n$ при этом отображении состоит из всех точек $\mathbb{P}_F^n$, лежащих вне «бесконечно удаленной гиперплоскости», которая есть множество классов эквивалентности упорядоченных наборов по $n+1$ элементов с нулевой x_0-координатой.

Эту гиперплоскость можно рассматривать как копию пространства $\mathbb{P}_F^{n-1}$ в силу взаимно однозначного соот-

ветствия

$$\text{класс } (0, x_1, \ldots, x_n) \longmapsto \text{класс } (x_1, \ldots, x_n).$$

(Например, если $n=2$, то проективная плоскость $\mathbb{P}^2_F$ представляется в виде объединения аффинной плоскости и «бесконечно удаленной проективной прямой».) Продолжая этот процесс, можно разложить $\mathbb{P}^n_F$ в несвязное объединение

$$\mathbb{A}^n_F \cup \mathbb{A}^{n-1}_F \cup \mathbb{A}^{n-2}_F \cup \ldots \cup \mathbb{A}^1_F \cup \text{точка}.$$

Однородным многочленом $\tilde{f}(X_0, \ldots, X_n) \in F[X_0, \ldots, X_n]$ степени d называется линейная комбинация мономов *одной и той же полной степени* d. Например, $X_0^3 + X_0^2X_1 - 3X_1X_2X_3 + X_3^3$ — однородный многочлен степени 3. Под *однородным пополнением* $\tilde{f}(X_0, X_1, \ldots, X_n)$ заданного многочлена $f(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$ степени d понимается многочлен

$$X_0^d f(X_1/X_0, \ldots, X_n/X_0),$$

который, очевидно, однороден и имеет степень d. Например, однородное пополнение для $X_3^3 - 3X_1X_2X_3 + X_1 + 1$ совпадает с приведенным выше примером однородного многочлена степени 3.

Если $\tilde{f}(X_0, \ldots, X_n)$ однороден и $\tilde{f}(x_0, \ldots, x_n) = 0$, то $\tilde{f}(\lambda x_0, \ldots, \lambda x_n) = 0$ для любого $\lambda \in F^\times$. Поэтому можно говорить о множестве точек (классов эквивалентности упорядоченных наборов из $n+1$ элементов) пространства $\mathbb{P}^n_F$, в которых $\tilde{f}$ обращается в нуль. Это множество точек $\tilde{H}_{\tilde{f}}$ называется *проективной гиперповерхностью*, заданной однородным уравнением $\tilde{f} = 0$ в $\mathbb{P}^n_F$.

Пусть $\tilde{f}(X_0, \ldots, X_n)$ — однородное пополнение многочлена $f(X_1, \ldots, X_n)$. Тогда $\tilde{H}_{\tilde{f}}$ называется *проективным замыканием* гиперповерхности H_f. С интуитивной точки зрения $\tilde{H}_{\tilde{f}}$ получается из H_f «присоединением точек, к которым H_f стремится на бесконечности». Например, если H_f — гипербола ($F = \mathbb{R}$)

$$\frac{X_1^2}{a^2} - \frac{X_2^2}{b^2} = 1,$$

то $\tilde{f}(X_0, X_1, X_2) = X_1^2/a^2 - X_2^2/b^2 - X_0^2$ и $\tilde{H}_{\tilde{f}}$ отождествляется с

$$\{(1, X_1, X_2) \mid X_1^2/a^2 - X_2^2/b^2 = 1\} \cup \{(0, 1, X_2) \mid X_2 = \pm b/a\},$$

т. е. это H_f плюс точки бесконечно удаленной прямой, соответствующие наклонам асимптот кривой H_f.

Пусть теперь K — произвольное поле, содержащее F. Если коэффициенты некоторого многочлена лежат в F, то они лежат и в K. Поэтому можно рассмотреть «K-точки» гиперповерхности H_f, т. е. множество

$$H_f(K) \overset{\text{def}}{=} \{(x_1, \ldots, x_n) \in \mathbb{A}_K^n \mid f(x_1, \ldots, x_n) = 0\}.$$

Аналогично определяется $\tilde{H}_{\tilde{f}}(K)$ для однородного многочлена $\tilde{f}(X_0, \ldots, X_n)$.

Далее мы работаем с конечными полями $F = \mathbb{F}_q$ и их конечными расширениями $K = \mathbb{F}_{q^s}$. В этой ситуации множества $H_f(K)$ и $\tilde{H}_{\tilde{f}}(K)$ конечны, так как $\mathbb{A}_K^n$ (и $\mathbb{P}_K^n$) состоят лишь из конечного числа точек. Для $\mathbb{A}_K^n$ это число наборов по n элементов из K, и оно равно q^{sn}. Фиксируем H_f (или $\tilde{H}_{\tilde{f}}$). В этом случае определена последовательность натуральных чисел $N_1, N_2, N_3, \ldots$, равных числу $\mathbb{F}_q$-точек, $\mathbb{F}_{q^2}$-точек, $\mathbb{F}_{q^3}$-точек, ... гиперповерхности H_f (или $\tilde{H}_{\tilde{f}}$), т. е.

$$N_s \overset{\text{def}}{=} \#(H_f(\mathbb{F}_{q^s})).$$

По любой заданной последовательности целых чисел, которая, как $\{N_s\}$, имеет геометрический или теоретико-числовой смысл, можно построить «производящую функцию», а именно некоторый степенной ряд, кодирующий всю информацию о данной последовательности $\{N_s\}$. Это так называемая «дзета-функция», определяемая как формальный степенной ряд

$$\exp\left(\sum_{s=1}^{\infty} N_s T^s/s\right) \in \mathbb{Q}[[T]].$$

Будем обозначать ее через $Z(H_f/\mathbb{F}_q; T)$, где $\mathbb{F}_q$ указывает на основное поле определения. Очевидно, постоянный член степенного ряда $Z(H_f/\mathbb{F}_q; T)$ равен 1.

Прежде чем перейти к примерам, докажем две элементарные леммы.

Лемма 1. *Коэффициенты ряда* $Z(H_f/\mathbb{F}_q; T)$ *лежат в* $\mathbb{Z}$.

Доказательство. Сопоставим каждой K-точке $P = (x_1, \ldots, x_n)$ из H_f (K — конечное расширение поля $\mathbb{F}_q$) наименьший показатель $s = s_0$, при котором все $x_i \in \mathbb{F}_{q^{s_0}}$. Пусть $P_j = (x_{1j}, \ldots, x_{nj})$, $j = 1, \ldots, s_0$, — все «сопряженные» с P точки, т. е. $x_{i1}, \ldots, x_{is_0}$ сопряжены с $x_i = x_{i1}$ над $\mathbb{F}_q$. Тогда точки P_j различны. Действительно, если все x_i остаются неподвижными при некотором нетривиальном автоморфизме σ поля $\mathbb{F}_{q^{s_0}}$ над $\mathbb{F}_q$, то они принадлежат меньшему полю (а именно полю σ-инвариантов $\{x \in \mathbb{F}_{q^{s_0}} \mid \sigma(x) = x\}$).

Вычислим теперь вклад точек $P_1, \ldots, P_{s_0}$ в $Z(H_f/\mathbb{F}_q; T)$. Каждая из них является $\mathbb{F}_{q^s}$-точкой в H_f тогда и только тогда, когда $\mathbb{F}_{q^s} \supset \mathbb{F}_{q^{s_0}}$, т. е. когда $s_0 \mid s$ (см. упр. 1 к § III.1). Итак, они вносят вклад, равный s_0, в N_{s_0}, N_{2s_0}, N_{3s_0}, ... Поэтому общий вклад этих точек в $Z(H_f/\mathbb{F}_q; T)$ равен

$$\exp\left(\sum_{j=1}^{\infty} s_0 T^{js_0}/js_0\right) = \exp(-\log(1 - T^{s_0})) =$$

$$= \frac{1}{1 - T^{s_0}} = \sum_{j=0}^{\infty} T^{js_0}.$$

Полная же дзета-функция представима в виде произведения рядов такого вида (причем лишь конечное число из них имеет нетривиальный T-член степени $\leqslant s_0$), а поэтому ее коэффициенты — целые числа. □

Замечание. Из доказательства видно, что эти коэффициенты, кроме того, неотрицательны.

Лемма 2. *Коэффициент при* T^j *в* $Z(H_f/\mathbb{F}_q; T)$ *не превосходит* q^{nj}.

Доказательство. Максимальное значение N_s равно $q^{ns} = \#\,\mathbb{A}^n_{q^s}$. Очевидно, все коэффициенты ряда $Z(H_f/\mathbb{F}_q; T)$ не превосходят соответствующих коэффициентов ряда,

полученного подстановкой в него q^{ns} вместо N_s. Но

$$\exp\left(\sum_{s=1}^{\infty} q^{ns}T^s/s\right) = \exp\left(-\log\left(1-q^nT\right)\right) = 1/(1-q^nT) = \sum_{j=0}^{\infty} q^{nj}T^j. \square$$

В качестве простого примера рассмотрим вычисление дзета-функции аффинной прямой $L = H_{X_1} \subset \mathbb{A}^2_{\mathbb{F}_q}$. Очевидно, $N_s = q^s$, поэтому

$$Z\left(L/\mathbb{F}_q;\ T\right) = \exp\left(\sum q^sT^s/s\right) = \exp\left(-\log\left(1-qT\right)\right) = \frac{1}{1-qT}.$$

Аналогично определяется дзета-функция проективной гиперповерхности, только при этом используется последовательность чисел

$$\tilde{N}_s \overset{\text{def}}{=} \#\left(\tilde{H}_{\tilde{f}}\left(\mathbb{F}_{q^s}\right)\right).$$

Так, например, для проективной прямой $\tilde{L}$ мы имеем $\tilde{N}_s = q^s + 1$, поэтому

$$Z\left(\tilde{L}/\mathbb{F}_q;\ T\right) = \exp\left(\sum\left(q^sT^s/s + T^s/s\right)\right) = \exp\left(-\log\left(1-qT\right) - \log\left(1-T\right)\right) = \frac{1}{(1-T)(1-qT)}.$$

Оказывается, гораздо естественнее работать с проективными гиперповерхностями, чем с аффинными.

Возьмем, например, единичную окружность $X_1^2 + X_2^2 = 1$, проективное замыкание которой $\tilde{H}_{\tilde{f}}$ задается уравнением $\tilde{f} = X_1^2 + X_2^2 - X_0^2 = 0$. В этом случае проще вычислить $Z\left(\tilde{H}_{\tilde{f}}/\mathbb{F}_q;\ T\right)$, чем $Z\left(H_f/\mathbb{F}_q;\ T\right)$, где $f = X_1^2 + X_2^2 - 1$. (Будем предполагать, что $p = \operatorname{char}\mathbb{F}_q \neq 2$.) Почему же это проще? А потому, что существует взаимно однозначное соответствие между $\tilde{H}_{\tilde{f}}(K)$ и $\tilde{L}(K)$ ($\tilde{L}$ обозначает проективную прямую). Для конструкции такого отображения рассмотрим проектирование из «южного полюса» на прямую $X_2 = 1$, как показано на рис. 1.

После несложных вычислений получается: $x_1 = 4t/(4+t^2)$, $x_2 = (4-t^2)/(4+t^2)$, а $t = 2x_1/(x_2+1)$. При переходе от t к x это отображение имеет неопределенность для $t^2 = -4$, т. е. для двух значений t в случае $q^s \equiv 1 \pmod 4$, а если $q^s \equiv 3 \pmod 4$, то таких значений t нет (см. упр. 8 к § III.1). Для обратного отображения тоже

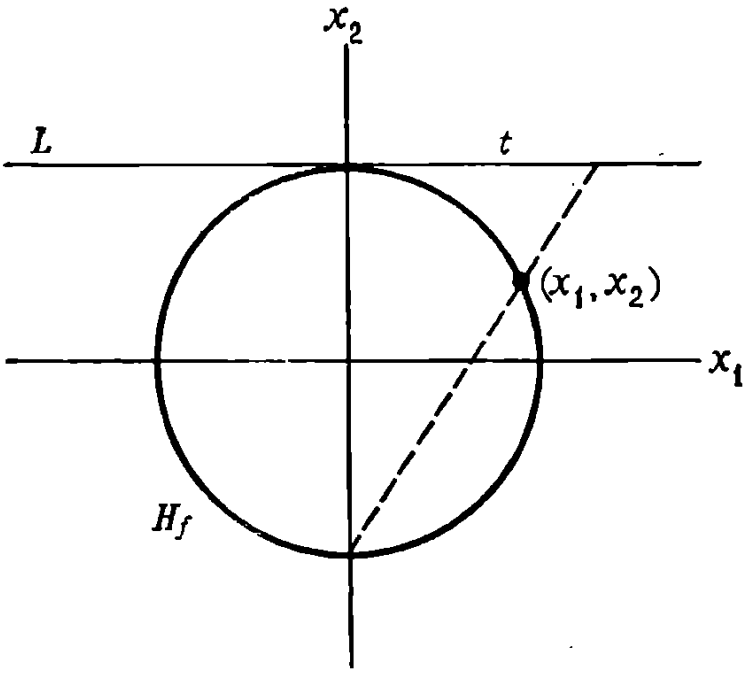


Рис. V.1.

возникает точка неопределенности с $x_2 = -1$ и $x_1 = 0$. Однако при переходе к проективным замыканиям окружности и прямой получается всюду определенное взаимно однозначное соответствие, задаваемое в однородных координатах (X_0, X_1, X_2) и (X'_0, X'_1) следующим образом:

$$(x'_0, x'_1) \longmapsto (4x'^2_0 + x'^2_1,\ 4x'_0x'_1,\ 4x'^2_0 - x'^2_1);$$

$$(x_0, x_1, x_2) \longmapsto \begin{cases} (x_2 + x_0, 2x_1), & \text{если } (x_2 + x_0, 2x_1) \neq (0, 0), \\ (0, 1), & \text{если } (x_2 + x_0, 2x_1) = (0, 0). \end{cases}$$

Читателю рекомендуется аккуратно проверить, что это действительно взаимно однозначное соответствие между проективной прямой и множеством классов эквивалентности упорядоченных троек (x_0, x_1, x_2), удовлетворяю-

щих уравнению $x_1^2+x_2^2-x_0^2=0$. Итак, поскольку $\tilde{N}_s$ одно и то же для $\tilde{H}_{\tilde{f}}$ и $\tilde{L}$, имеем

$$Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q;\ T)=Z(\tilde{L}/\mathbb{F}_q;\ T)=1/[(1-T)(1-qT)].$$

Если же мы хотим найти $Z(H_f/\mathbb{F}_q;\ T)$, $f=X_1^2+X_2^2-1$, следует вычесть из $\tilde{N}_s$ все точки «на бесконечности» для $\tilde{H}_{\tilde{f}}$, т. е. те, для которых $x_1^2+x_2^2=x_0^2$ и $x_0=0$. Таких точек ровно две, если -1 имеет квадратный корень в $\mathbb{F}_{q^s}$, и ни одной в противном случае.

Случай (1). Пусть $q\equiv 1 \pmod 4$. Тогда -1 всегда имеет квадратный корень в $\mathbb{F}_{q^s}$ (см. упр. 8 к § III.1), и $N_s=\tilde{N}_s-2$,

$$Z(H_f/\mathbb{F}_q;\ T)=\frac{Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q;\ T)}{\exp\left(\sum_{s=1}^{\infty}2T^s/s\right)}=\frac{1/[(1-T)(1-qT)]}{1/(1-T)^2}=\frac{1-T}{1-qT}.$$

Случай (2). Пусть $q\equiv 3 \pmod 4$. Тогда, как легко показать, $N_s=\tilde{N}_s$ при нечетных s и $N_s=\tilde{N}_s-2$ при четных s. Поэтому

$$Z(H_f/\mathbb{F}_q;\ T)=\frac{Z(\tilde{H}_f/\mathbb{F}_q;\ T)}{\exp\left(\sum_{s=1}^{\infty}2T^{2s}/2s\right)}=\frac{1/[(1-T)(1-qT)]}{1/(1-T^2)}=\frac{1+T}{1-qT}.$$

Заметим, что во всех примерах, как ниже в примерах из упражнений, дзета-функция оказывается рациональной функцией, т. е. отношением двух многочленов. Это важный общий факт. Его впервые доказал Дворк в 1960 г., остроумно применив методы p-адического анализа.

Теорема (Дворк). *Дзета-функция любой аффинной* (или проективной, см. ниже упр. 5) *гиперповерхности является отношением двух многочленов с коэффициентами в* $\mathbb{Q}$ (и даже в $\mathbb{Z}$ и постоянным членом 1, см. ниже упр. 13).

Оставшаяся часть главы посвящена доказательству этой теоремы, принадлежащему Дворку.

Отметим, что определение дзета-функции, данное выше для гиперповерхностей, допускает обобщение на более широкий класс объектов, включающий аффинные и проективные «алгебраические многообразия», которые определяются подобно гиперповерхностям, только уже не одним, а несколькими полиномиальными уравнениями. Теорема Дворка верна также и для алгебраических многообразий (см. ниже упр. 4).

Теорема Дворка имеет глубокие конкретные следствия в теории систем полиномиальных уравнений над конечными полями. Из нее следует существование такого конечного набора комплексных чисел $\alpha_1, \ldots, \alpha_t, \beta_1, \ldots, \beta_u$, что $N_s = \sum_{i=1}^{t} \alpha_i^s - \sum_{i=1}^{u} \beta_i^s$ для *любого* $s = 1, 2, 3, \ldots$ (см. ниже упр. 6). Иначе говоря, зная конечный набор данных (α_i и β_i), а эти данные определяются уже конечным набором чисел N_s, мы получаем простую формулу, предсказывающую *все* остальные N_s. Правда, для практического применения этой формулы необходимо знать верхнюю границу степени числителя и знаменателя нашей рациональной функции $Z(H/\mathbb{F}_q; T)$ (подробности см. ниже в упр. 7—9). На самом деле во всех важных случаях степень числителя и знаменателя дзета-функции известна, как и многое другое. Эта информация содержится в знаменитых гипотезах А. Вейля[1]) (недавно доказанных, но доказательство которых даже в простейших случаях выходит далеко за рамки этой книги).

Рациональность дзета-функции была частью серии гипотез, сформулированных Вейлем в 1949 г. Данное Дворком доказательство рациональности представляло собой первый важный шаг на пути к доказательству этих гипотез. Последний шаг в этом направлении — полученное в 1973 г. Делинем доказательство так называемой «гипотезы Римана» для алгебраических многообразий над конечным полем — явился кульминацией четвертьвековых напряженных исследований в этой области.

---

[1]) В настоящей книге речь идет исключительно о гипотезах Вейля, относящихся к случаю многообразий над конечным полем. — *Прим. перев.*

В случае *гладкой* проективной гиперповерхности $\tilde{H}_{\tilde{f}}$ (т. е. когда все частные производные $\tilde{f}$ по всем переменным не обращаются в нуль одновременно) гипотезы Вейля утверждают следующее:

(i) $Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q;\ T)=P(T)^{\pm 1}/((1-T)(1-qT)(1-q^2T)\dots$ $\dots(1-q^{n-1}T))$, где $P(T)\in 1+T\mathbb{Z}[T]$ имеет степень β, а β — число, определяемое «топологией» данной гиперповерхности (оно называется ее числом Бетти; если $\tilde{H}_{\tilde{f}}$ — кривая, то это удвоенный род («число ручек») соответствующей римановой поверхности). Здесь ± 1 означает, что мы берем $P(T)$ для четного n и $1/P(T)$ для нечетного n.

(ii) Если α — обратный корень многочлена $P(T)$, то тем же свойством обладает q^{n-1}/α.

(iii) Абсолютная величина каждого из обратных корней многочлена $P(T)$ равна $q^{(n-1)/2}$. (Это утверждение называется «гипотезой Римана» по аналогии с классической гипотезой Римана о нулях дзета-функции Римана; см. по этому поводу ниже упр. 15.)

Упражнения

1. Какова дзета-функция точки? Какова $Z\left(\mathbb{A}^n_{\mathbb{F}_q}/\mathbb{F}_q;\ T\right)$?

2. Вычислите $Z\left(\mathbb{P}^n_{\mathbb{F}_q}/\mathbb{F}_q;\ T\right)$.

3. Пусть $f(X_1, \dots, X_n)=X_n+g(X_1, \dots, X_{n-1})$, где $g\in$ $\in\mathbb{F}_q[X_1, \dots, X_{n-1}]$. Докажите, что

$$Z(H_f/\mathbb{F}_q;\ T)=Z\left(\mathbb{A}^{n-1}_{\mathbb{F}_q}/\mathbb{F}_q;\ T\right).$$

4. Пусть $f_1(X_1, \dots, X_n)$, $f_2(X_1, \dots, X_n)$, $\dots$, $f_r(X_1, \dots$ $\dots, X_n)\in\mathbb{F}_q[X_1, \dots, X_n]$, а $H_{\{f_1, f_2, \dots, f_r\}}(\mathbb{F}_{q^s})\subset\mathbb{A}^n_{\mathbb{F}_{q^s}}$ — множество наборов по n элементов из $\mathbb{F}_{q^s}$, которые удовлетворяют *всем* уравнениям $f_i=0$, $i=1, 2, \dots, r$:

$$H_{\{f_1, f_2, \dots, f_r\}}(\mathbb{F}_{q^s}) \overset{\text{def}}{=} \{(x_1, \dots, x_n)\in\mathbb{A}^n_{\mathbb{F}_{q^s}} \mid f_1(x_1, \dots, x_n)=\dots$$
$$\dots=f_r(x_1, \dots, x_n)=0\}.$$

Такое H называется (аффинным) алгебраическим многообразием. Пусть $N_s=\#H(\mathbb{F}_{q^s})$ (где H — сокращенное обозначение для

$H_{\{f_1, \ldots, f_r\}}$). Определим дзета-функцию, как и выше: $Z(H/\mathbb{F}_q; T) \underset{\text{def}}{=} \exp\left(\sum_{s=1}^{\infty} N_s T^s/s\right)$. Докажите, что из теоремы Дворка для аффинных гиперповерхностей следует теорема Дворка для аффинных алгебраических многообразий. (*Указание.* Пусть, скажем, $r=2$. Покажите, что тогда $\#H_{\{f_1,f_2\}}(\mathbb{F}_{q^s}) = \#H_{f_1}(\mathbb{F}_{q^s}) + \#H_{f_2}(\mathbb{F}_{q^s}) - \#H_{f_1 f_2}(\mathbb{F}_{q^s})$, где $H_{f_1 f_2}$ — гиперповерхность, заданная уравнением $f_1 \cdot f_2 = 0$.)

5. Докажите, что если теорема Дворка верна для аффинных гиперповерхностей, то она верна и для проективных гиперповерхностей.

6. Докажите, что теорема Дворка эквивалентна следующему утверждению: существует набор алгебраических комплексных чисел $\alpha_1, \ldots, \alpha_t, \beta_1, \ldots, \beta_u$, для которого каждое из α_i при сопряжении переходит в некоторое α_j, а каждое из β_i — в некоторое β_k и

$$N_s = \sum_{i=1}^{t} \alpha_i^s - \sum_{i=1}^{u} \beta_i^s \text{ для всех } s = 1, 2, 3, \ldots.$$

7. Известно, что дзета-функция гладкой проективной кубической кривой $\tilde{E} = \tilde{H}_{\tilde{f}}$ ($\dim \tilde{E} = 1$, $\deg \tilde{f} = 3$; $\tilde{E}$ называется *эллиптической кривой*) всегда представима в виде $(1 + aT + qT^2)/[(1-T)(1-qT)]$ для некоторого $a \in \mathbb{Z}$. Покажите, что если известно число точек в $\tilde{E}(\mathbb{F}_q)$, то можно найти: (1) a и (2) $\#\tilde{E}(\mathbb{F}_{q^s})$ при всех s.

8. Используя факт, сформулированный в предыдущем упражнении, найдите $Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q; T)$ для $f(X_1, X_2)$, равного:

(i) $X_2^3 - X_1^3 - 1$ и $q \equiv 2 \pmod 3$;
(ii) $X_2^2 - X_1^3 + X_1$ и $q \equiv 3 \pmod 4$, а также для $q = 5$, 13 и 9.

9. Предположим, что рациональность функции $Z(H/\mathbb{F}_q; T)$ уже известна. Пусть m и n — степени ее числителя и знаменателя соответственно. Докажите, что числа $N_s = \#H(\mathbb{F}_{q^s})$ для $s = 1, 2, 3, \ldots, m+n$ однозначно определяют все остальные N_s. (То есть две такие рациональные функции $\exp\left(\sum_{s=1}^{\infty} N_s T^s/s\right)$ и $\exp\left(\sum_{s=1}^{\infty} N'_s T^s/s\right)$, для которых $N_s = N'_s$ при $1 \leqslant s \leqslant m+n$, совпадают, а значит, и $N_s = N'_s$ для всех s.)

10. Вычислите $Z(H_f/\mathbb{F}_q; T)$ для трехмерной гиперповерхности H_f, заданной уравнением

$$X_1X_4 - X_2X_3 = 1.$$

11. Вычислите $Z(H_f/\mathbb{F}_q; T)$ и $Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q; T)$ ($\tilde{f}$ — однородное пополнение f) для кривой H_f, заданной уравнением:

(i) $X_1X_2 = 0$; (ii) $X_1X_2(X_1 + X_2 + 1) = 0$; (iii) $X_2^2 - X_1^2 = 1$;
(iv) $X_2^2 = X_1^3$; (v) $X_2^2 = X_1^3 + X_1^2$.

12. Прямые в $\mathbb{P}^3$ получаются как пересечение двух различных гиперповерхностей, т. е. прямая состоит из классов эквивалентности четверок, удовлетворяющих одновременно двум заданным однородным линейным уравнениям. Пусть N_s — число прямых в $\mathbb{P}^3_{\mathbb{F}_{q^s}}$. Используя данное выше определение дзета-функции по последовательности чисел N_s, вычислите дзета-функцию семейства прямых на трехмерном проективном пространстве.

13. Используя упр. 12 к § IV.4, докажите, что из приведенной выше леммы 1 и теоремы Дворка «с коэффициентами в $\mathbb{Q}$» следует теорема Дворка «с коэффициентами в $\mathbb{Z}$ и постоянным членом 1».

14. Пусть H_f — кривая, заданная уравнением $X_2^2 = X_1^5 + 1$, а $p \equiv 3$ или $7 \pmod{10}$. Докажите, что

$$Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_p; T) = \frac{1 + p^2T^4}{(1-T)(1-pT)}.$$

15. Пусть $\tilde{H}_{\tilde{f}}$ — гладкая проективная кривая. Предполагая справедливость гипотез Вейля для $Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q; T)$ (которые для кривых были доказаны гораздо раньше, чем в общем случае), покажите, что все нули аналитической функции

$$F(s) \underset{\text{def}}{=} Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q; q^{-s})$$

комплексного переменного s лежат на прямой $\operatorname{Re} s = 1/2$. Этот факт объясняет, почему гипотезу Вейля (iii) называют «гипотезой Римана».

§ 2. ХАРАКТЕРЫ И ИХ ПОДНЯТИЕ

Ω-значным характером на конечной группе G называется гомоморфизм группы G в мультипликативную группу $\Omega^\times$ ненулевых чисел из Ω. Так как $g^{\text{порядок элемента } g} = 1$ для любого $g \in G$, характер отображает G в множество корней из 1 поля Ω. Пусть, например, G — аддитивная группа поля $\mathbb{F}_p$, ε — корень степени p из 1 в Ω, и пусть $\tilde{a}$ — приведенный вычет

для $a \in \mathbb{F}_p$. Тогда отображение $a \longmapsto \varepsilon^{\hat{a}}$ является характером на $\mathbb{F}_p$. В дальнейшем будем писать $a \longmapsto \varepsilon^a$, опуская тильду. Если $\varepsilon \neq 1$, этот характер нетривиален, т. е. его образ состоит не только из 1.

Если $\mathbb{F}_q$ — конечное поле из $q = p^s$ элементов, то известно, что существует $s = [\mathbb{F}_q : \mathbb{F}_p]$ автоморфизмов $\sigma_0, \ldots, \sigma_{s-1}$ поля $\mathbb{F}_q$, для которых $\sigma_i(a) = a^{p^i}$, $a \in \mathbb{F}_q$ (см. упр. 6 к § III.1). Пусть $a \in \mathbb{F}_q$. *След* элемента a, обозначаемый $\operatorname{Tr} a$, определяется формулой

$$\operatorname{Tr} a \underset{\text{def}}{=} \sum_{i=0}^{s-1} \sigma_i(a) = a + a^p + a^{p^2} + \ldots + a^{p^{s-1}}.$$

Очевидно, $(\operatorname{Tr} a)^p = \operatorname{Tr}(a)$, т. е. $\operatorname{Tr} a \in \mathbb{F}_p$. Кроме того, $\operatorname{Tr}(a+b) = \operatorname{Tr} a + \operatorname{Tr} b$. Поэтому отображение

$$a \longmapsto \varepsilon^{\operatorname{Tr} a}$$

есть Ω-значный характер аддитивной группы поля $\mathbb{F}_q$.

Напомним, что каждому элементу $a \in \mathbb{F}_q$ соответствует единственный представитель Тейхмюллера $t \in \Omega$, который лежит в неразветвленном расширении K поля $\mathbb{Q}_p$, порожденном примитивным корнем из 1 степени $(q-1)$, причем $t^q = t$, а редукция t по модулю p равна a. Цель этого параграфа — найти p-адический степенной ряд $\Theta(T)$, значение которого при $T = t$ совпадало бы с $\varepsilon^{\operatorname{Tr} a}$. (Точнее, ряд $\Theta(T)\Theta(T^p)\Theta(T^{p^2})\ldots\Theta(T^{p^{s-1}})$, где $q = p^s$, будет принимать значение $\varepsilon^{\operatorname{Tr} a}$ при $T = t$.)

Фиксируем $a \in \mathbb{F}_q^\times$. Пусть $t \in K$ — соответствующий представитель Тейхмюллера. Обозначим через Tr_K отображение следа для элементов из K в $\mathbb{Q}_p$, переводящее элемент K в сумму сопряженных с ним над $\mathbb{Q}_p$. Тогда для представителя Тейхмюллера t (см. упр. 1 к § 4 ниже)

$$\operatorname{Tr}_K t = t + t^p + t^{p^2} + \ldots + t^{p^{s-1}} \in \mathbb{Z}_p,$$

а редукция $\operatorname{Tr}_K t$ по модулю p равна

$$a + a^p + a^{p^2} + \ldots + a^{p^{s-1}} = \operatorname{Tr} a \in \mathbb{F}_p.$$

Следовательно, $\varepsilon^{\operatorname{Tr} a} = \varepsilon^{\operatorname{Tr}_K t}$, поскольку возведение ε в некоторую степень из $\mathbb{Z}_p$ зависит только от класса вычетов по модулю p.

Пусть $\lambda = \varepsilon - 1$. Нам уже известно, что $\operatorname{ord}_p \lambda = 1/(p-1)$ (см. упр. 7 к § III.4). Хотим же мы найти p-адическое выражение, зависящее от t, для

$$(1+\lambda)^t + t^p + t^{p^2} + \ldots + t^{p^{s-1}} = \varepsilon^{\operatorname{Tr} a}.$$

Действуя наивно, можно было бы положить

$$g(T) = (1+\lambda)^T = \sum_{i=0}^{\infty} \frac{T(T-1)\ldots(T-i+1)}{i!}\lambda^i,$$

а затем построить ряд $g(T)\,g(T^p)\,g(T^{p^2})\ldots g(T^{p^{s-1}})$. Но тогда возникает следующая трудность: как придать смысл бесконечному ряду $g(T)$ для интересующих нас значений $T = t$? А именно, если $t \notin \mathbb{Z}_p$, т. е. вычет a не лежит в $\mathbb{F}_p$, то, очевидно, $|t-i|_p = 1$ для всех $i \in \mathbb{Z}$, откуда

$$\operatorname{ord}_p \frac{t(t-1)\ldots(t-i+1)}{i!}\lambda^i = i \operatorname{ord}_p \lambda - \frac{i - S_i}{p-1} = \frac{S_i}{p-1},$$

так что этот порядок не стремится к бесконечности.

Выход из положения заключается в использовании ряда $F(X, Y)$ с лучшей сходимостью, который был введен в конце § IV.2:

$$F(X, Y) = (1+Y)^X (1+Y^p)^{(X^p - X)/p} (1+Y^{p^2})^{(X^{p^2} - X^p)/p^2} \ldots$$
$$\ldots (1+Y^{p^n})^{(X^{p^n} - X^{p^{n-1}})/p^n} \ldots.$$

Напомним, что сомножители справа обозначают соответствующие биномиальные ряды из $\mathbb{Q}[[X, Y]]$. Рассмотрим теперь $F(X, Y)$ как степенной ряд от X при фиксированном Y:

$$F(X, Y) = \sum_{n=0}^{\infty} \left(X^n \sum_{m=n}^{\infty} a_{m,n} Y^m \right), \quad a_{m,n} \in \mathbb{Z}_p;$$

при этом использован тот факт, что $a_{m,n} \neq 0$ только для $m \geqslant n$. Действительно, каждое слагаемое ряда $B_{(X^{p^n} - X^{p^{n-1}})/p^n,\, p}(Y^{p^n})$, т. е.

$$\frac{X^{p^n} - X^{p^{n-1}}}{p^n}\left(\frac{X^{p^n} - X^{p^{n-1}}}{p^n} - 1\right)\ldots\left(\frac{X^{p^n} - X^{p^{n-1}}}{p^n} - i + 1\right)\frac{Y^{ip^n}}{i!}$$

после перемножения и приведения подобных членов

дает лишь члены, степень которых по X меньше или равна степени Y^{ip^n} по Y.

Напомним, что $\lambda=\varepsilon-1$, а $\operatorname{ord}_p\lambda=1/(p-1)$. Положим

$$\Theta(T)=F(T,\lambda)=\sum_{n=0}^{\infty}a_nT^n,$$

где $a_n=\sum_{m=n}^{\infty}a_{m,n}\lambda^m$. Очевидно, $\operatorname{ord}_p a_n\geqslant n/(p-1)$, так как каждый член в выражении для a_n делится на λ^n. В силу полноты поля $\mathbb{Q}_p(\varepsilon)=\mathbb{Q}_p(\lambda)$ имеет место включение $a_n\in\mathbb{Q}_p(\varepsilon)$, а $\Theta(T)\in\mathbb{Q}_p(\varepsilon)[[T]]$. Более того, $\Theta(T)$ сходится для всех значений $t\in D(p^{1/(p-1)-})$, потому что $\operatorname{ord}_p a_n\geqslant n/(p-1)$.

Рассмотрим теперь для фиксированного t ряд

$$(1+Y)^t+t^p+\ldots+t^{p^{s-1}}\overset{\text{def}}{=}B_{t+t^p+\ldots+t^{p^{s-1}},\,p}(Y).$$

Легко доказать следующее формальное тождество в $\Omega[[Y]]$:

$$(1+Y)^t+t^p+\ldots+t^{p^{s-1}}=F(t,Y)F(t^p,Y)\ldots F\left(t^{p^{s-1}},Y\right).$$

В самом деле, после тривиальных сокращений правая часть приводится к виду

$$(1+Y)^t+t^p+\ldots+t^{p^{s-1}}(1+Yp)^{(t^{p^s}-t)/p}\times$$
$$\times(1+Yp^2)^{(t^{p^{s+1}}-t^p)/p^2}(1+Yp^3)^{(t^{p^{s+2}}-t^{p^2})/p^3}\ldots.$$

Но $t^{p^s}=t$, и мы получаем требуемое.

Итак, при подстановке t вместо T в $\Theta(T)\Theta(T^p)\ldots\Theta\left(T^{p^{s-1}}\right)$ получается

$$F(t,\lambda)F(t^p,\lambda)\ldots F\left(t^{p^{s-1}},\lambda\right)=$$
$$=(1+\lambda)^t+t^p+\ldots+t^{p^{s-1}}=\varepsilon^{\operatorname{Tr}a}.$$

В результате мы нашли хороший p-адический степенной ряд $\Theta(T)=\sum a_nT^n\in\mathbb{Q}_p(\varepsilon)[[T]]$ с $\operatorname{ord}_p a_n\geqslant n/(p-1)$, такой, что значения характера $a\longmapsto\varepsilon^{\operatorname{Tr}a}$ на $\mathbb{F}_q$ вычисляются подстановкой поднятия Тейхмюллера для a в $\Theta(T)\Theta(T^p)\ldots\Theta\left(T^{p^{s-1}}\right)$. Ряд Θ можно рассматривать как «поднятие» этого характера аддитивной группы поля $\mathbb{F}_q$ до функции на Ω (точнее, на некото-

ром диске в Ω, включающем *замкнутый* единичный диск, а следовательно, и все представители Тейхмюллера).

Такие поднятия, как Θ, важны потому, что многие понятия анализа приложимы непосредственно только к p-адическим, а не к конечным полям. Если некоторый объект, связанный с конечным полем, например дзета-функция гиперповерхности над этим полем, допускает поднятие в поле p-адических чисел, то к нему уже можно применять анализ. В заключение отметим, как важно, что наше поднятие Θ сходится по крайней мере на *замкнутом* единичном диске (а, скажем, не просто открытом единичном диске): ведь точки, которые нас больше всего интересуют, — представители Тейхмюллера — лежат как раз на единичной окружности.

§ 3. ЛИНЕЙНЫЕ ОТОБРАЖЕНИЯ НА ВЕКТОРНОМ ПРОСТРАНСТВЕ СТЕПЕННЫХ РЯДОВ

Обозначим через R кольцо формальных степенных рядов над Ω от n независимых переменных:

$$R \underset{\text{def}}{=} \Omega[[X_1, X_2, \ldots, X_n]].$$

Моном $X_1^{u_1}X_2^{u_2}\ldots X_n^{u_n}$ будем обозначать через X^u, где $u=(u_1, \ldots, u_n)$ — упорядоченный набор из n целых неотрицательных чисел. Тогда каждый элемент из R можно записать в виде $\sum a_u X^u$, где u пробегает множество U всех упорядоченных наборов из n целых неотрицательных чисел и $a_u \in \Omega$.

Отметим, что R — бесконечномерное векторное пространство над Ω. Для каждого $G \in R$ определим линейное отображение из R в R, обозначаемое также через G, сопоставлением

$$r \longmapsto Gr,$$

т. е. это отображение умножения степенных рядов из R на некоторый фиксированный степенной ряд G.

Кроме того, для каждого целого положительного $q>1$ (в приложениях q будет степенью простого числа p) определим линейное отображение T_q: $R \to R$, полагая

$$r = \sum a_u X^u \longmapsto T_q(r) = \sum a_{qu} X^u,$$

где qu обозначает набор $(qu_1, qu_2, \ldots, qu_n)$. Например, при $n=1$ это отображение степенных рядов, при котором стираются все X^j-члены для j, не делящихся на q, а во всех X^j-членах, где $q \mid j$, X^j заменяется на $X^{j/q}$.

Положим теперь $\Psi_{q,G} \overset{\text{def}}{=} T_q \circ G$: $R \to R$. Пусть $G = \sum_{w \in U} g_w X^w$. Тогда $\Psi_{q,G}$ — линейное отображение, задаваемое на мономах X^u формулой

$$\Psi_{q,G}(X^u) = T_q\left(\sum_{w \in U} g_w X^{w+u}\right) = \sum_{v \in U} g_{qv-u} X^v.$$

(При этом если набор $qv-u$ не лежит в U, т. е. имеет отрицательную компоненту, то считается, что соответствующее g_{qv-u} равно нулю.)

Обозначим через $G_q(X)$ степенной ряд $G(X^q) = \sum_{w \in U} g_w X^{qw}$. Легко проверить следующее соотношение (см. ниже упр. 7):

$$G \circ T_q = T_q \circ G_q = \Psi_{q,G_q}.$$

Определим на U функцию $|\ |$ формулой $|u| = \sum_{i=1}^{n} u_i$. Пусть

$$R_0 \overset{\text{def}}{=} \Big\{G = \sum_{w \in U} g_w X^w \in R \mid \text{существует такое } M > 0, \text{ что } \operatorname{ord}_p g_w \geqslant M|w| \text{ для всех } w \in U\Big\}.$$

Нетрудно проверить замкнутость R_0 относительно умножения и инвариантность при отображении $G \longmapsto G_q$. Отметим, что каждый степенной ряд из R_0 сходится для всех значений переменных, лежащих в некотором диске, строго большем чем $D(1)$. Один из важных примеров ряда, принадлежащего R_0, дает $\Theta(aX^w)$, где a берется из $D(1)$, а X^w обозначает моном от переменных $X_1, \ldots, X_n$ (см. ниже упр. 2).

Пусть V — конечномерное векторное пространство над полем F, а $\{a_{ij}\}$ — матрица линейного отображения A: $V \to V$ в некотором базисе. Тогда след отображения A определяется как

$$\operatorname{Tr} A \overset{\text{def}}{=} \sum a_{ii},$$

т. е. как сумма элементов главной диагонали (эта сумма не зависит от выбора базиса; по поводу этого факта и других основных понятий и результатов линейной алгебры см. [(а) 2], гл. 6[1]). (Использование того же символа Tr, что и для следа элемента поля $\mathbb{F}_q$, не должно приводить к путанице, поскольку из контекста всегда будет ясно, о чем идет речь.) Если поле F обладает некоторой метрикой, можно ввести след *бесконечной* матрицы A, при условии что сумма $\sum_{i=1}^{\infty} a_{ii}$ сходится.

Лемма 3. *Пусть* $G \in R_0$, $\Psi = \Psi_{q,G}$. *Тогда* $\operatorname{Tr}(\Psi^s)$ *определен для* $s = 1, 2, 3, \ldots$ *и*

$$(q^s - 1)^n \operatorname{Tr}(\Psi^s) = \sum_{\substack{x \in \Omega^n, \\ x^{q^s-1} = 1}} G(x) \cdot G(x^q) \cdot G\left(x^{q^2}\right) \ldots G\left(x^{q^{s-1}}\right),$$

где $x = (x_1, \ldots, x_n)$, $x^{q^i} = \left(x_1^{q^i}, \ldots, x_n^{q^i}\right)$, *а* $x^{q^s-1} = 1$ *означает, что* $x_j^{q^s-1} = 1$ *для* $j = 1, 2, \ldots, n$.

Доказательство. Разберем прежде всего случай $s = 1$, а затем сведем к нему общий случай. Так как $\Psi(X^u) = \sum_{v \in U} g_{qv-u} X^v$, то

$$\operatorname{Tr} \Psi = \sum_{u \in U} g_{(q-1)u}$$

и ряд сходится по определению R_0.

Рассмотрим теперь правую часть равенства в лемме. Для $i = 1, 2, \ldots, n$ имеем

$$\sum_{\substack{x_i \in \Omega, \\ x_i^{q-1} = 1}} x_i^{w_i} = \begin{cases} q-1, & \text{если } q-1 \text{ делит } w_i, \\ 0 & \text{в остальных случаях} \end{cases}$$

(см. ниже упр. 6). Следовательно,

$$\sum_{\substack{x \in \Omega^n, \\ x^{q-1} = 1}} x^w = \prod_i \sum_{x_i^{q-1} = 1} x_i^{w_i} = \begin{cases} (q-1)^n, \text{ если } q-1 \text{ делит } w, \\ 0 \text{ в остальных случаях.} \end{cases}$$

[1]) См. также книгу И. М. Гельфанда [(а) 4], гл. II. — *Прим. перев.*

Отсюда

$$\sum_{x^{q-1}=1} G(x) = \sum_{w \in U} g_w \sum_{x^{q-1}=1} x^w =$$

$$= (q-1)^n \sum_{u \in U} g_{(q-1)u} = (q-1)^n \operatorname{Tr} \Psi,$$

что и доказывает лемму для $s = 1$.

Предположим теперь, что $s > 1$. Тогда

$$\Psi^s = T_q \circ G \circ T_q \circ G \circ \Psi^{s-2} = T_q \circ T_q \circ G_q \circ G \circ \Psi^{s-2} =$$
$$= T_{q^2} \circ G \cdot G_q \circ \Psi^{s-2} = T_{q^2} \circ T_q \circ (G \cdot G_q)_q \, G \circ \Psi^{s-3} =$$
$$= T_{q^3} \circ G \cdot G_q \cdot G_{q^2} \circ \Psi^{s-3} = \ldots = T_{q^s} \circ G \cdot G_q \cdot G_{q^2} \ldots G_{q^{s-1}} =$$
$$= \Psi_{q^s,\ G \cdot G_q \cdot G_{q^2} \ldots G_{q^{s-1}}}.$$

Итак, заменив q на q^s и G на $G \cdot G_q \cdot G_{q^2} \ldots G_{q^{s-1}}$, мы установим лемму в общем виде. □

Пусть A — некоторая $r \times r$-матрица с элементами в поле F, а T — независимая переменная. Тогда $(1 - AT)$ (где 1 обозначает $r \times r$-матрицу тождественного преобразования) является $r \times r$-матрицей с элементами в кольце $F[T]$. Эта матрица играет существенную роль при изучении линейного отображения на F^r, соответствующего A, потому что ее определитель, равный $\det(1 - At)$ для любого конкретного значения $t \in F$ переменной T, обращается в нуль тогда и только тогда, когда существует нетривиальный вектор $v \in F^r$, для которого $0 = (1 - At)v = v - tAv$, т. е. $Av = (1/t)v$. Иначе говоря, это происходит тогда и только тогда, когда $1/t$ есть собственное значение матрицы A. Если $A = \{a_{ij}\}$, то

$$\det(1 - AT) = \sum_{m=0}^{n} b_m T^m,$$

где

$$b_m = (-1)^m \sum_{\substack{1 \leqslant u_1, \ldots, u_m \leqslant r \\ \sigma\text{—перестановка} \\ \text{этих } u_i}} \operatorname{sgn}(\sigma)\, a_{u_1, \sigma(u_1)} \times$$

$$\times a_{u_2, \sigma(u_2)} \ldots a_{u_m, \sigma(u_m)}.$$

(Функция $\operatorname{sgn}(\sigma)$ принимает значение $+1$ или -1 в соответствии с тем, является ли данная перестановка σ

произведением четного или нечетного числа транспозиций.)

Предположим теперь, что $A = \{a_{ij}\}_{i,\ j=1}^{\infty}$ — бесконечная «квадратная» матрица, а $F = \Omega$. Тогда выражение для $\det(1 - AT)$ будет иметь смысл как формальный степенной ряд в $\Omega[[T]]$, если только выражения для b_m, которые теперь являются бесконечными рядами (условие «$\leqslant r$» на u_i отбрасывается), сходятся.

Применим это понятие к случаю, когда $A = \{g_{q\sigma - u}\}_{u,\ \sigma \in U}$ — «матрица» отображения $\Psi = T_q \cdot G$, где $G \in R_0$, т. е. $\operatorname{ord}_p g_w \geqslant M|w|$. Тогда p-адические порядки членов в выражении для b_m допускают следующую оценку:

$$\operatorname{ord}_p [g_{q\sigma(u_1)-u_1} \cdot g_{q\sigma(u_2)-u_2} \cdots g_{q\sigma(u_m)-u_m}] \geqslant$$
$$\geqslant M[|q\sigma(u_1) - u_1| + |q\sigma(u_2) - u_2| + \ldots + |q\sigma(u_m) - u_m|] =$$
$$= M\left[\sum q|\sigma(u_i)| - \sum |u_i|\right] = M(q-1)\sum |u_i|.$$

(Отметим, что если G — степенной ряд от n переменных, то каждое u_i есть набор n целых неотрицательных чисел: $u_i = (u_{i1}, \ldots, u_{in})$ и $|u_i| = \sum_{j=1}^{n} u_{ij}$.) Из этого видно, что

$$\operatorname{ord}_p b_m \to \infty \quad \text{при} \quad m \to \infty,$$
$$\frac{1}{m} \operatorname{ord}_p b_m \to \infty \quad \text{при} \quad m \to \infty.$$

Последнее верно, так как существует лишь конечное число n-наборов u с заданным значением $|u|$, а среднее для $|u|$ по конечному множеству *различных* u_i, т. е. $(1/m)\sum_{i=1}^{m} |u_i|$, стремится к ∞.

Это доказывает, что

$$\det(1 - AT) = \sum_{m=0}^{\infty} b_m T^m$$

корректно определен (т. е. ряд, задающий каждое b_m, сходится) и его радиус сходимости бесконечен.

Докажем теперь еще один важный вспомогательный результат, сначала для конечных матриц, а затем для

$\{g_{qv-u}\}$. А именно, в $\Omega[[T]]$ имеет место следующее тождество для формальных степенных рядов:

$$\det(1-AT)=\exp_p\left(-\sum_{s=1}^{\infty}\operatorname{Tr}(A^s)\,T^s/s\right).$$

Чтобы доказать это, напомним прежде всего два факта из теории матриц (см. [(а) 2], гл. 6 [1])). Определитель и след матрицы не меняются при сопряжении $A\longmapsto CAC^{-1}$ посредством обратимой матрицы C, т. е. они инвариантны относительно замены базиса. Кроме того, если основное поле алгебраически замкнуто, что верно, например, для Ω, то после подходящей замены базиса любая матрица может быть приведена к верхней треугольной матрице A (например, к канонической жордановой форме). Иначе говоря, последняя матрица не имеет ненулевых элементов ниже главной диагонали. Поэтому при доказательстве тождества без потери общности можно предполагать, что $A=\{a_{ij}\}_{i,\,j=1}^{r}$ верхняя треугольная. Тогда левая часть требуемого равенства принимает вид $\prod_{i=1}^{r}(1-a_{ii}T)$. Справа же стоит

$$\exp_p\left(-\sum_{s=1}^{\infty}\sum_{i=1}^{r}a_{ii}^sT^s/s\right)=\prod_{i=1}^{r}\exp_p\left(-\sum_{s=1}^{\infty}(a_{ii}T)^s/s\right)=$$

$$=\prod_{i=1}^{r}\exp_p(\log_p(1-a_{ii}T))=\prod_{i=1}^{r}(1-a_{ii}T),$$

поскольку $\operatorname{Tr}(A^s)=\sum_{i=1}^{r}a_{ii}^s$.

Разбор обобщения этого тождества на случай бесконечных матриц A мы оставим читателю в качестве упражнения (см. ниже упр. 8).

Резюмируем все это в следующей лемме.

Лемма 4. *Пусть* $G(X)=\sum_{w\in U}g_wX^w\in R_0$, *а* $\Psi=T_q\circ G$, *так что матрица отображения* Ψ *есть* $A=\{g_{qv-u}\}_{v,\,u\in U}$.

[1]) А также [(а) 4], гл. II и III. — *Прим. перев.*

Тогда ряд $\det(1 - AT)$ *из* $\Omega[[T]]$ *корректно определен, имеет бесконечный радиус сходимости и равен*

$$\exp_p\left\{-\sum_{s=1}^{\infty} \mathrm{Tr}\,(A^s)\,T^s/s\right\}.$$

§ 4. *p*-АДИЧЕСКОЕ АНАЛИТИЧЕСКОЕ ВЫРАЖЕНИЕ ДЛЯ ДЗЕТА-ФУНКЦИИ

В этом параграфе будет доказано, что дзета-функция

$$Z(H_f/\mathbb{F}_q;\ T) \in \mathbb{Z}[[T]] \subset \Omega[[T]]$$

любой гиперповерхности H_f, заданной уравнением $f = 0$ с $f(X_1, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_n]$, является отношением двух степенных рядов из $\Omega[[T]]$ с бесконечными радиусами сходимости. (В другой терминологии: является p-адической *мероморфной* функцией, или является отношением двух *целых* p-адических функций.)

Докажем это индукцией по числу переменных n (т. е. по размерности $n-1$ гиперповерхности H_f). При $n = 0$ (т. е. когда H_f пусто) утверждение тривиально. Предположим, что оно справедливо для $1, 2, \ldots, n-1$ переменных. Вместо того чтобы доказывать наше утверждение для

$$Z(H_f/\mathbb{F}_q;\ T) = \exp(\sum N_s T^s/s),$$

достаточно доказать его для

$$Z'(H_f/\mathbb{F}_q;\ T) \underset{\text{def}}{=} \exp\left(\sum_{s=1}^{\infty} N'_s T^s/s\right),$$

где

$N'_s \underset{\text{def}}{=}$ число n-наборов $(x_1, \ldots, x_n) \in \mathbb{F}_{q^s}^n$, для которых $f(x_1, \ldots, x_n) = 0$ *и* все x_i отличны от нуля $=$ $=$ число n-наборов $(x_1, \ldots, x_n) \in \mathbb{F}_{q^s}^n$, для которых

$$f(x_1, \ldots, x_n) = 0, \text{ а } x_i^{q^s - 1} = 1,\ i = 1, \ldots, n.$$

Действительно, чем отличается $Z'(H_f/\mathbb{F}_q;\ T)$ от $Z(H_f/\mathbb{F}_q;\ T)$? Очевидно,

$$Z(H_f/\mathbb{F}_q;\ T) = Z'(H_f/\mathbb{F}_q;\ T) \cdot \exp(\sum (N_s - N'_s)\,T^s/s),$$

причем экспоненциальный множитель в правой части есть дзета-функция объединения n гиперповерхностей H_i $(i=1, \ldots, n)$ меньшей [1]) размерности $(n-2)$, заданных уравнениями $f(X_1, \ldots, X_n)=0$ и $X_i=0$. Дзета-функция такого многообразия есть произведение дзета-функций для каждой H_i, *деленное* на произведение дзета-функций попарных пересечений H_i и H_j $(i \neq j)$ (т. е. $(n-3)$-мерных гиперповерхностей, заданных системой уравнений $X_i=X_j=0$ и $f(X_1, \ldots, X_n)=0$), *умноженное* на произведение дзета-функций тройных пересечений, *деленное* на произведение дзета-функций четверных пересечений, и т. д. Все эти дзета-функции p-адически мероморфны по предположению индукции [2]). Поэтому достаточно установить p-адическую мероморфность для Z', а отсюда уже будет следовать p-адическая мероморфность Z.

Фиксируем некоторое целое $s \geqslant 1$. Пусть $q=p^r$. Напомним, что если t обозначает представитель Тейхмюллера элемента $a \in \mathbb{F}_{q^s}$, то корень степени p из 1, равный $\varepsilon^{\mathrm{Tr}\, a}$, можно выразить через t при помощи p-адически аналитической функции

$$\varepsilon^{\mathrm{Tr}\, a}=\Theta(t)\,\Theta(t^p)\,\Theta(t^{p^2})\ldots\Theta(t^{p^{rs-1}}).$$

Одно из основных и просто доказываемых свойств характеров (см. ниже упр. 3—5) заключается в следующем:

$$\sum_{x_0 \in \mathbb{F}_{q^s}} \varepsilon^{\mathrm{Tr}\,(x_0 u)}=\begin{cases} 0, & \text{если } u \in \mathbb{F}_{q^s}^{\times}, \\ q^s, & \text{если } u=0, \end{cases}$$

или, после вычитания члена с $x_0=0$,

$$\sum_{x_0 \in \mathbb{F}_{q^s}^{\times}} \varepsilon^{\mathrm{Tr}\,(x_0 u)}=\begin{cases} -1, & \text{если } u \in \mathbb{F}_{q^s}^{\times}, \\ q^s-1, & \text{если } u=0. \end{cases}$$

[1]) Это верно лишь для достаточно общей гиперповерхности. Однако заметим, что если $\dim H_i > n-2$, то $H_i=\mathbb{A}^{n-1}_{\mathbb{F}_q}$, а в этом случае дзета-функция контролируема, так как хорошо известна. Это следует иметь в виду и в дальнейших рассуждениях. — *Прим. перев.*

[2]) Либо из их явного вида в случае многообразия $\mathbb{A}^{n-1}_{\mathbb{F}_q}$ (см. предыдущее примечание). — *Прим. перев.*

Применим это к функции $u=f(x_1, \ldots, x_n)$ и просуммируем результат по всем $x_1, \ldots, x_n \in \mathbb{F}_{q^s}^{\times}$. Получим

$$\sum_{x_0, x_1, \ldots, x_n \in \mathbb{F}_{q^s}^{\times}} \varepsilon^{\mathrm{Tr}(x_0 f(x_1, \ldots, x_n))} = q^s N_s' - (q^s-1)^n.$$

Заменим теперь все коэффициенты в $X_0 f(X_1, \ldots, X_n) \in \mathbb{F}_q[X_0, X_1, \ldots, X_n]$ их представителями Тейхмюллера; при этом получится многочлен $F(X_0, X_1, \ldots, X_n) = \sum_{i=1}^{N} a_i X^{\omega_i} \in \Omega[X_0, X_1, \ldots, X_n]$, где X^{ω_i} обозначает моном $X_0^{\omega_{i0}} X_1^{\omega_{i1}} \ldots X_n^{\omega_{in}}$, $\omega_i = (\omega_{i0}, \omega_{i1}, \ldots, \omega_{in})$. В этом случае

$$q^s N_s' = (q^s-1)^n + \sum_{x_0, x_1, \ldots, x_n \in \mathbb{F}_{q^s}^{\times}} \varepsilon^{\mathrm{Tr}(x_0 f(x_1, \ldots, x_n))} =$$

$$= (q^s-1)^n + \sum_{\substack{x_0, x_1, \ldots, x_n \in \Omega, \\ x_0^{q^s-1} = \ldots = x_n^{q^s-1} = 1}} \prod_{i=1}^{N} \Theta(a_i x^{\omega_i}) \times$$

$$\times \Theta(a_i^p x^{p\omega_i}) \ldots \Theta\left(a_i^{p^{rs-1}} x^{p^{rs-1}\omega_i}\right).$$

Заметим, что поскольку все коэффициенты многочлена $f(X_1, \ldots, X_n)$ лежат в $\mathbb{F}_q$, а $q=p^r$, то $a_i^{p^r} = a_i$. Положим теперь

$$G(X_0, \ldots, X_n) \overset{\text{def}}{=} \prod_{i=1}^{N} \Theta(a_i X^{\omega_i}) \Theta(a_i^p X^{p\omega_i}) \ldots \Theta\left(a_i^{p^{r-1}} X^{p^{r-1}\omega_i}\right).$$

Тогда

$$q^s N_s' = (q^s-1)^n + \sum_{\substack{x_0, x_1, \ldots, x_n \in \Omega \\ x_0^{q^s-1} = \ldots = x_n^{q^s-1} = 1}} G(x) \cdot G(x^q) \cdot G(x^{q^2}) \cdots G(x^{q^{s-1}}).$$

Так как каждый ряд $\Theta\left(a_i^{p^j} X^{p^j \omega_i}\right)$ принадлежит R_0 (см. ниже упр. 2), то это же справедливо для G:

$$G(X_0, \ldots, X_1) \in R_0 \subset \Omega[[X_0, \ldots, X_n]].$$

Следовательно, по лемме 3

$$q^s N'_s = (q^s - 1)^n + (q^s - 1)^{n+1} \operatorname{Tr}(\Psi^s),$$

т. е.

$$N'_s = \sum_{i=0}^{n} (-1)^i \binom{n}{i} q^{s(n-i-1)} + \sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} q^{s(n-i)} \operatorname{Tr}(\Psi^s).$$

Пусть (напомним, что A — матрица отображения Ψ)

$$\Delta(T) \underset{\text{def}}{=} \det(1 - AT) = \exp_p\left\{ - \sum_{s=1}^{\infty} \operatorname{Tr}(\Psi^s) T^s/s \right\}.$$

Тогда из предыдущего видно, что

$$\begin{aligned} Z'(H_f/\mathbb{F}_q;\ T) &= \exp_p\left\{ \sum_{s=1}^{\infty} N'_s T^s/s \right\} = \\ &= \prod_{i=0}^{n} \left[\exp_p\left\{ \sum_{s=1}^{\infty} q^{s(n-i-1)} T^s/s \right\} \right]^{(-1)^i \binom{n}{i}} \times \\ &\times \prod_{i=0}^{n+1} \left[\exp_p\left\{ \sum_{s=1}^{\infty} q^{s(n-i)} \operatorname{Tr}(\Psi^s) T^s/s \right\} \right]^{(-1)^i \binom{n+1}{i}} = \\ &= \prod_{i=0}^{n} (1 - q^{n-i-1})^{(-1)^{i+1} \binom{n}{i}} \prod_{i=0}^{n+1} \Delta(q^{n-i} T)^{(-1)^{i+1} \binom{n+1}{i}}. \end{aligned}$$

Каждый член последнего «альтернированного произведения» является целой p-адической функцией по лемме 4.

На этом завершается доказательство p-адической мероморфности дзета-функции — центральный результат в доказательстве теоремы Дворка. В следующем параграфе будет установлена представимость дзета-функции в виде отношения двух многочленов.

Упражнения

1. Пусть $t \in \Omega$ — примитивный корень степени $(p^s - 1)$ из 1. Докажите, что t, t^p, t^{p^2}, ..., $t^{p^{s-1}}$ исчерпывают все элементы, сопряженные с t над $\mathbb{Q}_p$. Другими словами, сопряженные с представителем Тейхмюллера элемента $a \in \mathbb{F}_q$ совпадают с представителями Тейхмюллера сопряженных с a элементов над $\mathbb{F}_p$.

2. Пусть $a \in D(1)$, а $X^{\omega} = X_1^{\omega_1} \dots X_n^{\omega_n}$. Докажите, что $\Theta(aX^{\omega}) \in R_0$.

3. Пусть $\sigma_1, \dots, \sigma_s$ — различные автоморфизмы поля K. Докажите, что не существует нетривиальных комбинаций $\sum a_i\sigma_i$, для которых $\sum a_i\sigma_i(x) = 0$ при любом $x \in K$. (*Указание*: воспользуйтесь индукцией по числу ненулевых a_i; в случае затруднений см. книгу Ленга [(а) 3], стр. 238.) Выведите отсюда, что отображение следа Tr из $\mathbb{F}_q$ в $\mathbb{F}_p$ ненулевое.

4. Пусть $\varepsilon \in \Omega$ — примитивный корень степени p из 1. Докажите, что $\sum\limits_{x \in \mathbb{F}_q} \varepsilon^{\mathrm{Tr}\, x} = 0$. (*Указание*: произведите замену $x \longmapsto x + x_0$, где $x_0 \in \mathbb{F}_p$ имеет ненулевой след.)

5. Докажите, что

$$\sum_{x \in \mathbb{F}_{q^s}^{\times}} \varepsilon^{\mathrm{Tr}(xu)} = \begin{cases} -1, & \text{если } u \in \mathbb{F}_{q^s}^{\times}, \\ q^s - 1, & \text{если } u = 0. \end{cases}$$

6. Докажите, что для любых целых положительных n и a

$$\sum_{\zeta \in \Omega,\, \zeta^n = 1} \zeta^a = \begin{cases} n, & \text{если } n \text{ делит } a, \\ 0 & \text{в противном случае.} \end{cases}$$

7. В обозначениях § 3 докажите, что $G \circ T_q = T_q \circ G_q$.

8. Распространите тождество

$$\det(1 - AT) = \exp_p\left(-\sum_{s=1}^{\infty} \mathrm{Tr}(A^s)\, T^s/s\right)$$

на бесконечные матрицы A при подходящих предположениях о сходимости следов.

9. *Задача на повторение.* Пусть $f(X) = \sum\limits_{i=0}^{n} a_i X^i \in \mathbb{F}_q[X]$ — многочлен от одной переменной с коэффициентами в $\mathbb{F}_q$, $q = p^r$, и ненулевым постоянным членом. Предположим, что нам надо найти число N различных корней многочлена $f(X)$ в $\mathbb{F}_q$. Обозначим через A_i представитель Тейхмюллера элемента a_i, $i = 0, \dots, n$. Пусть $\varepsilon = 1 + \lambda$ — фиксированный примитивный корень из 1 степени p в Ω, а $\Theta(T)$ — ряд из § 2. Положим

$$G(X, Y) = \prod_{i=0}^{n} \prod_{j=0}^{r-1} \Theta\left(A_i^{p^j} X^{ip^j} Y^{p^j}\right).$$

Докажите, что

$$N = \frac{q-1}{q} + \frac{1}{q} \sum_{\substack{x,\, y \in \Omega, \\ x^{q-1} = y^{q-1} = 1}} G(x, y).$$

§ 5. КОНЕЦ ДОКАЗАТЕЛЬСТВА

Теорема Дворка теперь легко выводится из следующего критерия представимости степенного ряда в виде рациональной функции.

Лемма 5. *Пусть* $F(T)=\sum_{i=0}^{\infty} a_i T^i \in K[[T]]$, *где* K — *произвольное поле. Целым числам* m, $s \geqslant 0$ *сопоставим матрицу* $A_{s,m}=\{a_{s+i+j}\}_{0 \leqslant i,\ j \leqslant m}$:

$$\begin{pmatrix} a_s & a_{s+1} & a_{s+2} & \cdots & a_{s+m} \\ a_{s+1} & a_{s+2} & a_{s+3} & \cdots & a_{s+m+1} \\ a_{s+2} & a_{s+3} & a_{s+4} & \cdots & a_{s+m+2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{s+m} & a_{s+m+1} & a_{s+m+2} & \cdots & a_{s+2m} \end{pmatrix}.$$

Пусть $N_{s,m} \overset{\text{def}}{=} \det(A_{s,m})$. *Тогда ряд* $F(T)$ *равен отношению двух многочленов*

$$F(T)=\frac{P(T)}{Q(T)}, \quad P(T),\ Q(T) \in K[T],$$

в том и только том случае, когда существуют целые $m \geqslant 0$ *и* S, *для которых* $N_{s,m}=0$ *при всяком* $s \geqslant S$.

Доказательство. Предположим вначале, что $F(T)$ есть такое отношение. Пусть $P(T)=\sum_{i=0}^{M} b_i T^i$, а $Q(T)=\sum_{i=0}^{N} c_i T^i$. Тогда, приравнивая коэффициенты при T^i в соотношении $F(T)\cdot Q(T)=P(T)$ для $i>\max(M, N)$, получим

$$\sum_{j=0}^{N} a_{i-N+j} c_{N-j}=0.$$

Пусть $S=\max(M-N+1, 1)$, а $m=N$. Возьмем $s \geqslant S$ и запишем эти уравнения для $i=s+N, s+N+1, \ldots, s+2N$:

$$\begin{aligned} a_s c_N + a_{s+1} c_{N-1} + \ldots + a_{s+N} c_0 &= 0, \\ a_{s+1} c_N + a_{s+2} c_{N-1} + \ldots + a_{s+N+1} c_0 &= 0, \\ \ldots\ldots\ldots\

Следовательно, матрица коэффициентов при c_j, равная $A_{s,N}$, имеет нулевой определитель:

$$N_{s,m} = N_{s,N} = 0 \quad \text{для } s \geqslant S.$$

Обратно, предположим, что $N_{s,m} = 0$ при $s \geqslant S$, где m выбрано минимальным с данным свойством: $N_{s,m} = 0$ при всех $s \geqslant S$. Утверждается, что $N_{s,m-1} \neq 0$ для *всех* $s \geqslant S$.

Предположим противное. Тогда некоторая нетривиальная линейная комбинация первых m строк r_0, $r_1, \ldots, r_{m-1}$ матрицы $A_{s,m}$ обращается в нуль везде, кроме, может быть, последнего столбца. Пусть r_{i_0} — первая строка с ненулевым коэффициентом в этой линейной комбинации, т. е. i_0-я строка r_{i_0} равна

$$\alpha_1 r_{i_0+1} + \alpha_2 r_{i_0+2} + \ldots + \alpha_{m-i_0-1} r_{m-1},$$

кроме, может быть, элемента последнего столбца. Заменим r_{i_0} в $A_{s,m}$ на $r_{i_0} - (\alpha_1 r_{i_0+1} + \ldots + \alpha_{m-i_0-1} r_{m-1})$ и рассмотрим следующие две возможности:

(1) $i_0 > 0$. Тогда мы получаем матрицу вида

$$\left(\begin{array}{cccc} a_s & a_{s+1} & \cdots & a_{s+m} \\ \hline a_{s+1} & a_{s+2} & \cdots & a_{s+m+1} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots\ 0 & \beta \\ \vdots & \vdots & & \vdots \\ a_{s+m} & a_{s+m+1} & \cdots & a_{s+2m} \end{array}\right)$$

и определитель выделенной матрицы равен $N_{s+1,m-1} = 0$.

(2) $i_0 = 0$. Тогда мы получаем

$$\left(\begin{array}{c|ccc|c} 0 & 0 & \cdots & 0 & \beta \\ \hline a_{s+1} & a_{s+2} & \cdots & & a_{s+m+1} \\ \vdots & \vdots & & & \vdots \\ a_{s+m} & a_{s+m+1} & \cdots & & a_{s+2m} \end{array}\right)$$

В этом случае $N_{s+1,m-1}$ совпадает с определителем каждой из двух выделенных матриц. Поскольку определитель $N_{s,m}$ всей матрицы равен 0, то либо определитель нижней выделенной матрицы равен 0, либо $\beta = 0$

и определитель верхней выделенной матрицы равен 0. Поэтому $N_{s+1,\,m-1}=0$.

Итак, в любом случае $N_{s+1,\,m-1}=0$. Далее по индукции легко получить, что $N_{s',\,m-1}=0$ при всех $s'\geqslant s$. Это противоречит минимальности выбранного m.

Но тогда при любом $s\geqslant S$ мы имеем $N_{s,\,m}=0$ и $N_{s,\,m-1}\neq 0$. Следовательно, существует линейная комбинация строк матрицы $A_{s,\,m}$, равная строке из нулей. Более того, у *этой комбинации коэффициент последней строки отличен от нуля.* Таким образом, последняя строка матрицы $A_{s,\,m}$ при любом $s\geqslant S$ представима в виде линейной комбинации предыдущих m строк. Поэтому всякое решение линейной системы

$$\begin{gathered}a_S u_m+a_{S+1}u_{m-1}+\ldots+a_{S+m}u_0=0,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ a_{S+m-1}u_m+a_{S+m}u_{m-1}+\ldots+a_{S+2m-1}u_0=0\end{gathered}$$

является решением уравнения

$$a_{S+m}u_m+a_{S+m+1}u_{m-1}+\ldots+a_{S+2m}u_0=0,$$

а по индукции — любого линейного уравнения

$$a_s u_m+a_{s+1}u_{m-1}+\ldots+a_{s+m}u_0=0$$

при $s\geqslant S$. Из этого, очевидно, следует, что

$$\left(\sum_{i=0}^{m}u_iX^i\right)\cdot\left(\sum_{i=1}^{\infty}a_iX^i\right)$$

— многочлен (степени $<S+m$). □

Закончим теперь доказательство теоремы, используя лемму 5. Нам понадобится «p-адическая подготовительная теорема Вейерштрасса» (теорема 14, § IV.4) в следующей форме: если $F(T)$ — целая p-адическая функция, то для любого положительного вещественного R (равного рациональной степени p) существует многочлен $P(T)$ и p-адический степенной ряд $F_0(T)\in 1+T\Omega[[T]]$, который сходится на диске $D(R)$ радиуса R *вместе со своим обратным* $G(T)$, а $F(T)=P(T)\cdot F_0(T)$. Действительно, положите в теореме 14 $p^\lambda=R$; так как F целая, она сходится на $D(p^\lambda)$.

Для краткости будем писать $\mathrm{Z}(T)$ вместо $\mathrm{Z}(H_f/\mathbb{F}_q; T)$. В § 4 мы выяснили, что $\mathrm{Z}(t) = A(T)/B(T)$, где $A(T)$ и $B(T)$ — две целые p-адические функции. Выберем некоторое $R > q^n$; для простоты возьмем, например, $R = q^{2n}$. Применим теперь утверждение предыдущего абзаца к $B(T)$. Получим, что $B(T) = P(T)/G(T)$, где $G(T)$ сходится на $D(R)$. Пусть $F(T) = A(T) \cdot G(T)$. Этот ряд также сходится на $D(R)$. Итак,

$$F(T) = P(T) \cdot \mathrm{Z}(T).$$

Пусть $F(T) = \sum_{i=0}^{\infty} b_i T^i \in 1 + T\Omega[[T]]$, $P(T) = \sum_{i=0}^{e} c_i T^i \in$ $\in 1 + T\Omega[T]$, $\mathrm{Z}(T) = \sum_{i=0}^{\infty} a_i T^i \in 1 + T\mathbb{Z}[[T]]$. По лемме 2 из § 1

$$|a_i|_\infty \leqslant q^{in}.$$

Поскольку $F(T)$ сходится на $D(R)$, то для достаточно большого i

$$|b_i|_p \leqslant R^{-i} = q^{-2ni}.$$

Фиксируем некоторое $m > 2e$. Пусть $A_{s,m} = \{a_{s+i+j}\}_{0 \leqslant i,\ j \leqslant m}$, как и выше, а $N_{s,m} = \det(A_{s,m})$. Утверждается, что для данного m мы имеем $N_{s,m} = 0$ при всех достаточно больших s. По лемме 5 отсюда будет следовать рациональность функции $\mathrm{Z}(T)$.

Приравнивая коэффициенты в соотношении $F(T) = P(T)\mathrm{Z}(T)$, находим

$$b_{j+e} = a_{j+e} + c_1 a_{j+e-1} + c_2 a_{j+e-2} + \ldots + c_e a_j.$$

Добавим в матрице $A_{s,m}$ к каждому $(j+e)$-му столбцу, начиная с последнего и двигаясь влево до e-го столбца, линейную комбинацию e предыдущих с коэффициентом c_k при $(j+e-k)$-м столбце. Тогда получится матрица, e первых столбцов которой те же, что и у $A_{s,m}$, а в остальных столбцах элементы a заменены соответствующими b. Определитель этой матрицы по-прежнему равен $N_{s,m}$. Используя ее вид, оценим $|N_{s,m}|_p$.

Так как $a_i \in \mathbb{Z}$, имеем $|a_i|_p \leqslant 1$. Поэтому $|N_{s,m}|_p \leqslant \left(\max_{i \geqslant s+e} |b_j|_p\right)^{m+1-e} < R^{-s(m+1-e)}$ для достаточно больших s. Но $R = q^{2n}$, а $m > 2e$, откуда $|N_{s,m}|_p < q^{-ns(m+2)}$.

С другой стороны, грубая оценка прямо для матрицы $A_{s,m}$ дает неравенство $|N_{s,m}|_\infty \leqslant (m+1)!\, q^{n(s+2m)(m+1)} = (m+1)!\, q^{2nm(m+1)} q^{ns(m+1)}$. Перемножая две указанные оценки, мы видим, что произведение p-адической нормы и обычной абсолютной величины для $N_{s,m}$ ограничено сверху выражением, которое меньше 1 при достаточно больших s:

$$|N_{s,m}|_p \cdot |N_{s,m}|_\infty < q^{-ns(m+2)} \cdot (m+1)!\, q^{2nm(m+1)} q^{ns(m+1)} = \frac{(m+1)!\, q^{2nm(m+1)}}{q^{ns}} < 1$$

при достаточно больших s. Однако $N_{s,m} \in \mathbb{Z}$, а единственное целое число n с этим свойством: $|n| \cdot |n|_p < 1$, есть число $n = 0$. Следовательно, $N_{s,m} = 0$ для всех достаточно больших s.

Таким образом, $Z(T)$ — рациональная функция и теорема Дворка доказана. □

ЛИТЕРАТУРА

Порядок работ внутри каждого из следующих пунктов приблизительно соответствует возрастанию их трудности. Для книг и больших статей это весьма грубая оценка, основанная главным образом на уровне подготовки, необходимой для понимания тех разделов, которые тесно связаны с материалом одной из наших глав I — V. [Работы, отмеченные звездочкой, добавлены при переводе. — *Перев.*]

(a) Подготовительная

1. Симмонс (Simmons G.) Introduction to topology and modern analysis. — McGraw-Hill, 1963.
2. Херстейн (Herstein I.) Topics in algebra. — John Wiley and Sons, 1975.
3. Ленг С. Алгебра. Пер. с англ. — М.: Мир, 1968.
4*. Гельфанд И. М. Лекции по линейной алгебре. — М.: Наука, 1966.
5*. Рудин У. Основы математического анализа. Пер. с англ. — М.: Мир, 1966.
6*. Куратовский К. Топология. Пер. с англ. — М.: Мир, т. 1, 1966; т. 2, 1969.

(b) Общая

1. Боревич З. И., Шафаревич И. Р. Теория чисел. — М.: Наука, 1964.
2. Ленг С. Алгебраическая теория чисел. Пер. с англ. — М.: Мир, 1966.
3. Серр Ж.-П. Курс арифметики. Пер. с франц. — М.: Мир, 1972.
4. Айрленд и Розен (Ireland K. and Rosen M.) Elements of number theory, including an introduction to equations over finite fields. — Bogden and Quigley, 1972.
5. Дынкин Е. Б., Успенский В. А. Математические беседы. — М.: Гостехиздат, 1952.
6. Малер (Mahler K.) Introduction to p-adic numbers and their functions. — Cambridge University Press, 1973.
7. Бахман (Bachman G.) Introduction to p-adic numbers and valuation theory. — Academic Press, 1964.
8. Монна (Monna A. F.) Analyse non-archimédienne. — Springer-Verlag, 1970.

(c) К главе II

1. Ивасава (Iwasawa K.) Lectures on p-adic L-functions. — Princeton University Press, 1972.
2. Кубота и Леопольдт (Kubota T., Leopoldt H. W.) Eine p-adische Theorie der Zetawerte I. — *J. Reine Angew. Math.*, **214/215** (1964), 328—339.
3. Катц (Katz N.) p-adic L-functions via moduli of elliptic curves. — Proceedings A. M. S. Summer Institute of Alg. Geom. at Arcata, Calif., 1974.
4. Ленг С. Введение в теорию модулярных форм. Пер. с англ. — М.: Мир, 1979.
5. Серр (Serre J.-P.) Formes modulaires et fonctions zêta p-adiques.

In: Modular functions of one variable III (Lecture Notes in Math. 350). — Springer-Verlag, 1973.

6. Манин Ю. И. Периоды параболических форм и p-адическне ряды Гекке. — *Матем. сб.*, **92** (1973), № 3, 378—400. (Особо отметим § 8.)

7. Вишик М. М. Неархимедовы меры, связанные с рядами Дирихле. — *Матем. сб.*, **99** (141) (1976), № 2, 248—266.

8. Амис и Велю (Amice Y., Vélu J.) Distributions p-adiques associées aux séries de Hecke. — Journées arithmétiques, 1974.

9. Катц (Katz N.) p-adic properties of modular schemes and modular forms. In: Modular functions of one variable III (Lecture Notes in Math. 350). — Springer-Verlag, 1973.

10. Катц (Katz N.) The Eisenstein measure and p-adic interpolation. — *Amer. J. Math.*, **99** (1977), 238—311.

11. Катц (Katz N.) p-adic interpolation of real analytic Eisenstein series. — *Ann. of Math.*, **104** (1976), 459—571.

12. Мазур и Суинертон-Дайер (Mazur B., Swinnerton-Dyer S.) Arithmetic of Weil curves. — *Invent. Math.*, **25** (1974), 1—61.

(d) К главе IV

1. Дворк (Dwork B.) § 1 из: On zeta function of a hypersurface. — *Publ. Math. I. H. E. S.*, **12** (1962), 7—17.

2. Амис (Amice Y.) Les nombres p-adiques. — Presses Universitaires de France, 1975.

(e) К главе V

1. Вейль (Weil A.) Number of solutions of equations in finite fields. — *Bull. Amer. Math. Soc.*, **55** (1949), 497—508.

2. Серр (Serre J.-P.) Rationalité des fonctions ζ des variétés algébriques (d'aprés Bernard Dwork). — Séminaire Bourbaki, No. 198, February 1960.

3. Дворк Б. О рациональности дзета-функции алгебраического многообразия. Пер. с англ. — Сб. *Математика*, **5:6** (1961), 55—72.

4. Монски (Monsky P.) p-adic analysis and zeta functions. Lectures at Kyoto University. — Kinokuniya Book Store, Tokyo, or Brandeis Univ. Math. Dept., 1970.

5. Катц (Katz N.) Une formule de congruence pour la fonction ζ. — S. G. A. 7 II (Lecture Notes in Math. 340), Springer-Verlag, 1973.

6. Дворк (Dwork B.) On the zeta function of a hypersurface. — *Publ. Math. I. H. E. S.*, **12** (1962), 5—68.

7. Дворк (Dwork B.) On the zeta function of a hypersurface II. — *Ann. of Math.*, **80** (1964), 227—299.

8. Дворк (Dwork B.) A deformation theory for the zeta function of a hypersurface. — Proc. Int. Cong. Math. 1962 Stockholm, 247—259.

9. Катц Н. Работы Дворка. Пер. с франц. — Сб. *Математика*, **18:6** (1974), 3—19.

ОГЛАВЛЕНИЕ

ГЛАВА I. p-АДИЧЕСКИЕ ЧИСЛА 9

§ 1. Основные понятия 9
§ 2. Метрики поля рациональных чисел 10
Упражнения 17
§ 3. Как строится поле комплексных чисел 19
§ 4. Поле p-адических чисел 21
§ 5. Арифметика в $\mathbb{Q}_p$ 29
Упражнения 34

ГЛАВА II. p-АДИЧЕСКАЯ ИНТЕРПОЛЯЦИЯ ДЗЕТА-ФУНКЦИИ РИМАНА 37

§ 1. Формула для значений $\zeta(2k)$ 39
§ 2. p-адическая интерполяция функции $f(s)=a^s$ . . 44
Упражнения 48
§ 3. p-адические распределения 51
Упражнения 55
§ 4. Распределения Бернулли 57
§ 5. Меры и интегрирование 59
Упражнения 66
§ 6. p-адическая ζ-функция как преобразование Мелина — Мазура 67
§ 7. Краткий обзор (без доказательств) 75
Упражнения 80

ГЛАВА III. КОНСТРУКЦИЯ ПОЛЯ Ω 82

§ 1. Конечные поля 82
Упражнения 90
§ 2. Продолжение норм 91
Упражнения 103
§ 3. Алгебраическое замыкание поля $\mathbb{Q}_p$ 104
§ 4. Поле Ω 112
Упражнения 115

ГЛАВА IV. p-АДИЧЕСКИЕ СТЕПЕННЫЕ РЯДЫ 118

§ 1. Элементарные функции 118
§ 2. Экспонента Артина — Хассе 129
Упражнения 136
§ 3. Многоугольники Ньютона в случае многочленов 141

§ 4. Многоугольники Ньютона в случае степенных рядов 144
Упражнения 156

ГЛАВА V. РАЦИОНАЛЬНОСТЬ ДЗЕТА-ФУНКЦИИ СИСТЕМЫ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ НАД КОНЕЧНЫМ ПОЛЕМ 159

§ 1. Гиперповерхности и их дзета-функции 159
Упражнения 167
§ 2. Характеры и их поднятне 169
§ 3. Линейные отображения на векторном пространстве степенных рядов 173
§ 4. p-адическое аналитическое выражение для дзета-функции 179
Упражнения 182
§ 5. Конец доказательства 184

Литература 189

Н. Коблиц

p-АДИЧЕСКИЕ ЧИСЛА
p-АДИЧЕСКИЙ АНАЛИЗ
И ДЗЕТА-ФУНКЦИИ

Ст. научный редактор Н. И. Плужникова
Мл. научный редактор Л. А. Королева
Художник А. В. Шипов
Художественный редактор В. И. Шаповалов
Технические редакторы Н. Д. Толстякова, Н. И. Борисова
Корректор Е. К. Монякова

ИБ № 2217

Сдано в набор 18.05.81. Подписано к печати 07.01.82. Формат 84×108¹/₃₂. Бумага типографская № 1. Объем 3,00 бум. л. Усл. печ. л. 10,08. Усл. кр.-отт. 10,28. Уч.-изд. л. 8,43. Изд. № 1/0787. Тираж 7900 экз. Заказ 1153. Цена 65 коп.

Издательство «Мир»
129820, Москва, И-110, ГСП 1-й Рижский пер., 2.

Набрано и сматрицировано в ордена Октябрьской Революции, ордена Трудового Красного Знамени Ленинградском производственно-техническом объединении «Печатный Двор» имени А. М. Горького Союзполиграфпрома при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли. 197136, Ленинград, П-136, Чкаловский пр., 15. Отпечатано в Ленинградской типографии № 2 головном предприятии ордена Трудового Красного Знамени Ленинградского объединения «Техническая книга» им. Евгении Соколовой Союзполиграфпрома при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли. 198052, г. Ленинград, Л-52, Измайловский проспект, 29.